



EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

THIRD SECTION

CASE OF KANEV AND BULGARIAN HELSINKI COMMITTEE v. BULGARIA

(Application no. 45864/22)

JUDGMENT

Art 8 • Private life • Correspondence • Refusal of State Agency for National Security to disclose whether it gathered intelligence on the applicants or held information to that effect in its databases • Lack of effective safeguards providing a minimum degree of protection against arbitrary and unlawful processing by the Agency of data • Interference not in accordance with a “law”

Prepared by the Registry. Does not bind the Court.

STRASBOURG

28 April 2026

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

TABLE OF CONTENTS

INTRODUCTION.....	1
THE FACTS	2
I. BACKGROUND.....	2
II. JUNE 2021 REQUEST MADE TO THE AGENCY.....	2
A. The request for information and the Agency’s response to it.....	2
B. Judicial review of the Agency’s refusal to disclose the information.....	4
1. Proceedings before the Sofia City Administrative Court	4
(a) Course of the proceedings.....	4
(b) Judgment of the Sofia City Administrative Court	5
2. Appeal proceedings before the Supreme Administrative Court	6
(a) Course of the proceedings.....	6
(b) Judgment of the Supreme Administrative Court.....	6
III. REQUEST TO THE NATIONAL BUREAU	8
IV. JUDICIAL REVIEW OF THE AGENCY’S OFFICIAL-SECRETS RULE.....	8
V. JUNE 2023 REQUEST TO THE AGENCY.....	9
A. The request and the Agency’s response to it	9
B. Judicial review of the Agency’s refusal to disclose the information.....	10
1. Proceedings before the Sofia City Administrative Court	10
2. Appeal proceedings before the Supreme Administrative Court	10
C. Renewed proceedings before the Agency.....	11
VI. INFORMATION REQUEST BY THE GOVERNMENT AGENT	12
RELEVANT LEGAL FRAMEWORK AND PRACTICE	12
I. BULGARIAN DOMESTIC LAW AND PRACTICE.....	12
A. State Agency for National Security Act 2007	12
1. The Agency, its tasks and powers.....	12
2. Informers recruited by the Agency	14
3. Personal data processed by the Agency	14
(a) Access to personal data processed by the Agency.....	15
(i) Relevant statutory provisions and regulations	15
(ii) Case-law of the Bulgarian courts under those provisions.....	16
(α) 2012 case	16
(β) 2014-18 case.....	16
(γ) 2021-22 case.....	17
(b) Supervision of the processing of personal data by the Agency	17
4. General supervision of the Agency’s work.....	17
(a) By Parliament.....	17
(b) By the Government	18
(c) By the President of the Republic.....	18
B. Special Surveillance Means Act 1997	18

C.	Protection of Personal Data Act 2002	19
1.	Scope of application.....	20
(a)	<i>Ratione personae</i>	20
(b)	Application to processing for national security purposes	20
2.	Right to access personal data and restrictions on that right.....	21
(a)	In relation to processing falling within the scope of the GDPR	21
(b)	In relation to processing by the authorities for law-enforcement purposes	21
3.	Supervisory authority.....	22
4.	Remedies.....	24
(a)	In respect of processing falling within the scope of the GDPR	24
(b)	In respect of processing undertaken by the authorities for law-enforcement purposes	24
D.	Protection of Classified Information Act 2002.....	24
1.	Types of classified information	24
2.	Time-limits for protecting classified information.....	25
3.	Access to classified information by lawyers and litigants.....	25
(a)	Relevant provisions of the Act.....	25
(b)	Case-law and practice of the administrative courts under sections 39(3)(3) and 39a of the Protection of Classified Information Act 2002.....	26
E.	Management and Functioning of the System for Safeguarding National Security Act 2015	27
II.	EUROPEAN UNION (EU) LAW.....	28
A.	Treaty on European Union	28
B.	Treaty on the Functioning of the European Union	28
C.	Charter of Fundamental Rights of the European Union	28
D.	General Data Protection Regulation	29
1.	Scope of application <i>ratione materiae</i>	30
2.	Right to access personal data	30
3.	Restrictions to the right of access	30
4.	Supervisory authority.....	31
5.	Remedies.....	32
E.	Law Enforcement Directive.....	32
1.	Scope of application <i>ratione materiae</i>	33
2.	Right to access personal data	33
3.	Restrictions on the right of access	34
4.	Indirect exercise of the right of access.....	35
5.	Supervisory authority.....	36
6.	Remedies.....	37

III. COUNCIL OF EUROPE INSTRUMENTS.....	38
A. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data	38
B. Additional Protocol to the 1981 Convention	39
C. Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data	40
1. Duty to give effect	40
2. Right of access and exceptions to that right	40
3. Obligation to demonstrate compliance	41
4. Powers of the supervisory authorities.....	41
5. Remedies.....	42
6. Application of the amending Protocol on a provisional basis	42
IV. OTHER RELEVANT INTERNATIONAL MATERIAL.....	42
A. Relevant Reports.....	42
1. Report by the Venice Commission	42
2. Reports by the EU Agency for Fundamental Rights	44
B. Relevant Decision of the Committee of Ministers of the Council of Europe...	47
THE LAW.....	48
I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION.....	48
A. Admissibility	48
1. Compatibility <i>ratione materiae</i>	48
(a) The parties' submissions.....	48
(b) The Court's assessment.....	48
2. Exhaustion of domestic remedies	51
(a) The parties' submissions.....	51
(b) The Court's assessment.....	52
(i) First branch of the non-exhaustion objection.....	52
(ii) Second branch of the non-exhaustion objection	52
(iii) Third branch of the non-exhaustion objection	53
(iv) Conclusion	54
3. The Court's conclusion on the admissibility of the complaint	54
B. Merits.....	54
1. Existence of an interference with rights protected under Article 8 of the Convention.....	54
(a) The parties' submissions.....	54
(b) The Court's assessment.....	55
2. Justification for the interference	56
(a) The parties' submissions.....	56
(b) The Court's assessment.....	56
(i) Was the interference "in accordance with the law"?	56
(α) General principles.....	56

KANEV AND BULGARIAN HELSINKI COMMITTEE v. BULGARIA JUDGMENT

(β) Application of those principles.....	59
– Judicial review of the Agency’s refusal to disclose whether it was processing data relating to the applicants	60
– Supervision by the Commission for the Protection of Personal Data.....	62
– Supervision by the National Bureau	63
– Supervision by a special parliamentary committee and the Parliament as a whole	64
– Supervision by the government and the President of the Republic.....	64
– Conclusion	64
(ii) Purpose and necessity of the interference	65
(iii) Final conclusion	65
II. ALLEGED PROCESSING OF DATA ABOUT THE APPLICANTS’ POLITICAL OPINIONS, AFFILIATIONS AND ACTIVITIES	65
A. The parties’ submissions	65
B. The Court’s assessment	66
III. ALLEGED BREACH OF THE RIGHT TO RECEIVE INFORMATION	66
A. The parties’ submissions	67
1. The Government	67
2. The applicants	67
B. The Court’s assessment	68
IV. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION.....	68
A. The parties’ submissions	68
B. The Court’s assessment	69
V. APPLICATION OF ARTICLE 41 OF THE CONVENTION.....	69
A. Damage	69
1. The applicants’ claim and the Government’s comments on it.....	69
2. The Court’s assessment	70
B. Costs and expenses	71
1. The applicants’ claim and the Government’s comments on it.....	71
(a) The claim and the documents produced in support of it	71
(b) The Government’s comments	71
2. The Court’s assessment	72
(a) Postage	72
(b) Domestic costs	72
(c) Lawyers’ fees	73
(d) Recapitulation	73
OPERATIVE PROVISIONS	73
JOINT DISSENTING OPINION OF JUDGES PAVLI AND NÍ RAIFEARTAIGH ..	75

In the case of Kanev and Bulgarian Helsinki Committee v. Bulgaria,

The European Court of Human Rights (Third Section), sitting as a Chamber composed of:

Ioannis Ktistakis, *President*,

Peeter Roosma,

Darian Pavli,

Úna Ní Raifeartaigh,

Mateja Đurović,

Vasilka Sancin, *judges*,

Mira Raycheva, *ad hoc judge*,

and Milan Blaško, *Section Registrar*,

Having regard to:

the application (no. 45864/22) against the Republic of Bulgaria lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms (“the Convention”) by a Bulgarian national, Mr Krasimir Ivanov Kanev, and an association having its registered office in Bulgaria, the Bulgarian Helsinki Committee (“the applicants”), on 19 September 2022;

the decision to give the Bulgarian Government (“the Government”) notice of the application;

the parties’ observations;

the decision of the special committee composed within the Fifth Section of the Court to consider the Government’s request under Rule 44F § 2 of the Rules of Court in relation to a classified document produced by them;

the decision of the President of the Section to exempt Diana Kovatcheva, the judge elected in respect of Bulgaria, from sitting in this case and his ensuing decision to appoint Mira Raycheva to sit as *ad hoc* judge in the case; and

the decision by a Chamber of the Section to reject the applicants’ request for the recusal of Mira Raycheva, the *ad hoc* judge appointed in the case;

Having deliberated in private on 27 January and 17 March 2026,

Delivers the following judgment, which was adopted on the last-mentioned date:

INTRODUCTION

1. Following official revelations of wide-ranging covert surveillance of politicians and civil-society activists carried out by, among other authorities, Bulgaria’s State Agency for National Security (“the Agency”) in 2020-21, the two applicants – respectively, a well-known association for the defence of human rights and its chairperson – asked the Agency whether it had gathered intelligence on them and recruited any of the association’s members or staff as informers. The Agency refused to disclose such information and the administrative courts upheld its decision.

2. The main issue in the case is whether that refusal – seen against the background of allegedly well-founded suspicions that the Agency was abusing its broad surveillance powers, and the alleged absence of effective supervision of how it processes data acquired as a result of its operations – was in breach of Article 8 of the Convention.

THE FACTS

3. The first applicant, Mr Kanev, was born in 1958 and lives in Sofia. The second applicant, the Bulgarian Helsinki Committee (“the Committee”), is an association founded in 1992 with a registered office in Sofia. At the relevant time, Mr Kanev was the Committee’s chairperson. Both applicants were represented by Ms A. Kachaunova, a lawyer practising in Sofia.

4. The Government were represented by their Agent, Ms I. Stancheva-Chinova of the Ministry of Justice.

I. BACKGROUND

5. In mid-2021 the then caretaker Minister of Internal Affairs – who had in 2013-18 been head of the National Bureau for the Oversight of Special Means of Surveillance (“the National Bureau”; for details about that body, see *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, §§ 14-16 and 108-24, 11 January 2022) – stated publicly that several authorities, including the Agency, had been covertly intercepting “nearly round the clock” the communications of many people, including politicians and civil-society activists, who had taken part in a prolonged series of protests against the previous government and the Chief Prosecutor held in the second half of 2020 and early 2021. Although the Minister said that he was aware of the names of the people who had been targeted by that surveillance, he did not reveal them, except for that of the new caretaker Prime Minister.

II. JUNE 2021 REQUEST MADE TO THE AGENCY

A. The request for information and the Agency’s response to it

6. Referring to the revelations outlined in paragraph 5 above, in June 2021 Mr Kanev sent the Agency a letter requesting information on:

(a) whether it had used “special means of surveillance” (for the definition of that term in Bulgarian law, see *Ekimdzhiev and Others*, cited above, § 11) with respect to him personally, or to members or staff of the Committee, or to lawyers acting on its behalf; and

(b) whether intelligence-gathering methods or techniques had been used with respect to the Committee or any of its members or staff, and whether any

of the Committee's members or staff had been recruited as informers over the previous ten years or earlier.

7. In late June 2021 the Agency replied that in so far as the request concerned "special means of surveillance", that part of the request was to be addressed to the National Bureau. The amount of information about the use of such means and the way in which it could be obtained had been laid down in section 34g of the Special Surveillance Means Act 1997 ("the 1997 Act" – see *Ekimdzhiev and Others*, cited above, § 130; see also paragraph 82 (e) below). In so far as the request concerned other intelligence-gathering methods or techniques and the recruitment of informers, it touched on the existence (or otherwise) of data in the Agency's databases, access to which was governed by section 36(4) of the State Agency for National Security Act 2007 ("the 2007 Act") and regulations issued by the head of the Agency in 2009 (see paragraphs 67-72 below). The request fell short of the requirements of those regulations, according to which such a request (a) was to be lodged at the Agency's premises, and (b) contain precise information about the identity of the person lodging it.

8. In an amended request lodged with the Agency at the end of June 2021, Mr Kanev asked whether its databases contained information on (a) whether intelligence-gathering methods or techniques had been used with respect to him or the Committee, which he represented, and (b) whether any members or staff of the Committee had been recruited as Agency informers throughout the previous ten years or earlier. He referred to section 36(4) of the 2007 Act (see paragraph 67 below).

9. In mid-July 2021 the Agency replied that it refused to disclose such information, citing section 36(7) of the 2007 Act and the corresponding regulation (see paragraphs 69-70 below).

10. The Agency stated that it gathered intelligence by using specific methods and techniques, but also by "special means of surveillance" and through private persons collaborating with it. Information about all of those practices was classified. The techniques that it used to gather intelligence were set out in government regulations, and those were likewise classified. All responses to queries regarding information stored in its databases were classified as well. The only means of obtaining information about the use of "special means of surveillance" was set out in section 34g of the 1997 Act, and such requests were to be addressed to the National Bureau (see paragraphs 5 and 7 above, and paragraph 82 (e) below).

11. So far as the request concerned information about members and staff of the Committee, the 2007 Act barred the Agency from disclosing information about other people, unless those people had authorised the person seeking the information to do so on their behalf. Moreover, by section 23(3) of that Act the identities, personal data and work of the Agency's informers were to be kept secret. By section 23(4), such information could be communicated only to the courts or the prosecuting authorities in connection

with a specific criminal case, in keeping with the requirements of the Protection of Classified Information Act 2002 (see paragraph 61 below), and only after the informers in question had agreed to that.

B. Judicial review of the Agency's refusal to disclose the information

1. Proceedings before the Sofia City Administrative Court

(a) Course of the proceedings

12. Mr Kanev, acting both in his personal capacity and on behalf of the Committee, sought judicial review under section 36(9) of the 2007 Act (see paragraph 72 below) of the Agency's decision to withhold the information he was seeking. He also referred to several other statutes, in particular the Protection of Personal Data Act 2002 (see paragraph 84 below).

13. He contended that not all information kept by the Agency was a "State secret" or an "official secret" (for the definitions of those terms in Bulgarian law, see paragraphs 107-109 below). It was therefore absurd, and contrary to section 36(4) of the 2007 Act (see paragraph 67 below) – which enshrined the right to access personal data processed by the Agency – to state that all responses from queries regarding information in its databases were classified. Moreover, according to this Court's case-law, persons placed under covert surveillance were to be notified of that fact after that surveillance had ended, and both the collection and retention of data obtained in that way could constitute a breach of the Convention. Not only individuals but also legal persons could seek such information, because their Convention rights – in particular, the right to respect for one's "correspondence" – could likewise be affected by covert surveillance. Such surveillance could clearly be used to safeguard national security, but that term could easily be construed by the authorities in an unduly expansive way. A potential misuse of the surveillance system could infringe his right to respect for his private life and both his and the Committee's right to respect for their correspondence. One also had to consider the background against which he had made his request: the Court had already found that the covert surveillance system in Bulgaria was being overused, and the statements of the caretaker Minister of Internal Affairs (see paragraph 5 above) had rekindled the public's misgivings on that point.

14. In his claim for judicial review, Mr Kanev also asked the Sofia City Administrative Court to direct the Agency to produce (a) the order issued by the Agency's head (required under section 32 of the 2007 Act – see paragraph 109 *in fine* below) which listed the categories of information due to be classified as being an "official secret", and (b) any personal data of his that was being processed by the Agency. According to Mr Kanev, the court would be able to examine the Agency's decision properly only if it had that evidence before it.

15. In response to the claim for judicial review, in October 2021 the Agency produced a May 2020 order issued by its head setting out the categories of information held by the Agency that were to be classified as constituting an “official secret”. Point 14 of the schedule to that order specified that one of those categories was “data resulting from checks in the [Agency’s] databases containing classified information, in the event that those data fall short of a State secret” (for the definitions of the terms “official secret” and “State secret” in Bulgarian law, see paragraphs 107-109 below). According to the Agency, the information sought by the applicants had been properly withheld because it fell within the ambit of that point. In so far as the information concerned the personal data of other people, it could not be disclosed, except to authorities safeguarding national security, to the judicial authorities for the purposes of a specific criminal case, or to foreign authorities (if so required under an international treaty to which Bulgaria was party).

16. A month later, in November 2021, Mr Kanev brought separate proceedings for judicial review of the above-mentioned point 14 of the schedule (see paragraphs 32-39 below).

17. The Sofia City Administrative Court did not direct the Agency to produce data relating to Mr Kanev (as he had requested – see paragraph 14 (b) above), and the Agency did not do so.

18. In additional written submissions, Mr Kanev argued, in particular, that the Agency’s refusal to disclose the information that he had sought had not been properly justified with reference to specific impediments to its disclosure. He also pointed out that by law information marked as an “official secret” could remain classified for six months only; the Agency had not clarified when that period had started to run in his case.

(b) Judgment of the Sofia City Administrative Court

19. In November 2021 the Sofia City Administrative Court dismissed the claim for judicial review. It noted that Article 15(1) of the General Data Protection Regulation (see paragraphs 132 and 137 below) enshrined the right of access to personal data, but that under section 37a of the Protection of Personal Data Act 2002 (see paragraph 92 below) that right could be restricted by law. The law providing for the restriction in the case at hand was section 36(7) of the 2007 Act (see paragraph 70 below), which listed five grounds on which the Agency could refuse to give access to personal data. Those included safeguarding “State secrets” and “official secrets”, the sources of the information, and the covert methods or techniques for gathering it. The information sought by Mr Kanev could be seen as an “official secret”, as defined in point 14 of the schedule mentioned in paragraph 15 above (whose lawfulness the court could not review in those proceedings). It was within the Agency’s discretion to assess whether the disclosure of that information could compromise classified information or its

work. That was why section 36(8) of the 2007 Act (see paragraph 71 below) required the Agency to set out only the legal grounds for its refusal to disclose such information. So far as the request had concerned Agency informers, it had been fully justified to turn it down, since the Agency could only disclose such information to other authorities in limited circumstances (*печ. № 6820 от 19.11.2021 г. по адм. д. № 8299/2021 г., АС-София-град*).

2. Appeal proceedings before the Supreme Administrative Court

(a) Course of the proceedings

20. Mr Kanev appealed against the Sofia City Administrative Court's judgment, again acting both in a personal capacity and on behalf of the Committee.

21. Mr Kanev contended, in particular, that it remained unclear why the information that he had sought was to be viewed as an "official secret". Personal data could not be classified information, since that would render nugatory the statutory right to obtain access to such data. The Protection of Personal Data Act 2002 (see paragraphs 84-105 below) enshrined an unqualified right for data subjects to obtain from data controllers confirmation as to whether their personal data were being processed, and information about the purposes of that processing; the Agency had fully disregarded that Act. It also remained unclear on which of the five grounds listed in section 36(7) of the 2007 Act (see paragraph 70 below) the Agency had based its refusal to disclose the information he had sought. Mr Kanev also reiterated that information marked as "official secret" could remain classified for six months only, and that the Agency had not explained when that period had started to run in his case. He went on to argue that by omitting to direct the Agency to produce the personal data pertaining to him that it was processing, and then deciding whether the refusal to disclose those data had been justified only after seeing them (see paragraphs 14 (b) and 17 above), the Sofia City Administrative Court had infringed the rules of procedure. Lastly, Mr Kanev referred to this Court's case-law under Article 8 of the Convention that related to the protection of personal data (including the processing of such data by security agencies) and covert surveillance.

22. In late June 2022 Mr Kanev asked the Supreme Administrative Court to stay the proceedings pending the determination of his claim for judicial review of point 14 of the schedule mentioned in paragraph 15 above. At that time, those proceedings were pending on appeal before a five-judge panel of the same court (see paragraphs 33-34 below).

(b) Judgment of the Supreme Administrative Court

23. In a final judgment of 6 July 2022 (*печ. № 6724 от 06.07.2022 г. по адм. д. № 2157/2022 г., ВАС, V о.*), the Supreme Administrative Court upheld the Sofia City Administrative Court's judgment.

24. It found that that court's omission to direct the Agency to produce the information sought by Mr Kanev (see paragraphs 14 (b) and 17 above) had been fully in line with the rules of procedure, since the whole case revolved precisely around the question whether that information was to be disclosed – whereas Mr Kanev had in effect sought to obtain its disclosure through that request for evidence. All that was required from the courts in proceedings for judicial review of the Agency's refusal to disclose such information was to assess whether that refusal was lawful.

25. The Supreme Administrative Court noted that the Agency could process personal data in the exercise of its statutory information-processing tasks (see paragraph 60 below). The 2007 Act did not define "personal data", but the definition of the term could be found in Article 4(1) of Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("General Data Protection Regulation" – "the GDPR") (see paragraphs 132-133 below). Under section 36(4) of the 2007 Act (see paragraph 67 below), anyone could request access to personal data that related to him or her and were being processed in the Agency's databases without his or her knowledge. However, Mr Kanev's request to the Agency had in effect concerned its intelligence-gathering methods rather than any personal data collected by it. As the Agency had stated in its response to Mr Kanev, information about those methods was classified, and the Agency had therefore correctly refused to disclose it. As regards specifically "special means of surveillance", the only authority which could disclose whether such means had been used was the National Bureau (see paragraph 5 above and paragraph 82 (d) below). Given that it had been possible for Mr Kanev to approach the Bureau himself, the Agency's refusal to disclose information could not be viewed as infringing Article 8 of the Convention.

26. For the Supreme Administrative Court, it had also been proper for the Agency not to disclose who had been recruited by it as an informer. By section 23(3)(3) of the 2007 Act (see paragraph 61 below), the identities and personal data of people who had collaborated with the Agency were to remain secret. They could only be disclosed to the national security authorities or the judicial authorities in connection with a specific criminal case.

27. Lastly, the court found that there was no reason to stay the proceedings while awaiting the adjudication of Mr Kanev's claim for judicial review of point 14 of the schedule referred to in paragraph 15 above (see also paragraphs 32-39 below). That adjudication could not affect the lawfulness of the Agency's refusal to disclose the information sought by him, since the Agency itself had not referred to that provision in refusing his request; only the lower court had referred to it, and that had been an error – which had, however, not affected the overall correctness of the lower court's judgment.

III. REQUEST TO THE NATIONAL BUREAU

28. In June 2021, concurrently with his information request to the Agency (see paragraph 6 above), Mr Kanev lodged a request for information with the National Bureau asking whether “special means of surveillance” had been used throughout the previous ten years with respect to him personally or with respect to members or staff of the Committee or lawyers acting on its behalf.

29. In mid-June 2021 the National Bureau instructed Mr Kanev to rectify his request by giving his personal identification number and his address. It also advised him that it could check whether “special means of surveillance” had been used with respect to members, staff or lawyers of the Committee only if each of the people concerned requested such information in relation to himself or herself. Also, as prescribed by section 34g of the 1997 Act (see paragraph 82 (e) below), the Bureau would inform people that “special means of surveillance” had been used with respect to them only if that had been done unlawfully.

30. In late June 2021 Mr Kanev rectified his request, in line with those instructions.

31. In early July 2021 the National Bureau sent letters to the five authorities empowered under Bulgarian law to deploy “special means of surveillance” (see paragraph 82 (c) below), asking them whether they had done so with respect to Mr Kanev. Three of those authorities – the military intelligence service of the Ministry of Defence, the State Intelligence Agency, and the Ministry of Internal Affairs – replied in the negative. The replies of the two other authorities – the Agency and the Technical Operations Agency – were classified. Having reviewed all of those replies, on 3 August 2021 the Bureau informed Mr Kanev that its enquiries had not indicated that “special means of surveillance” had been used unlawfully against him.

IV. JUDICIAL REVIEW OF THE AGENCY’S OFFICIAL-SECRETS RULE

32. In November 2021 Mr Kanev, acting solely in his personal capacity, asked the Supreme Administrative Court either to declare point 14 of the schedule mentioned in paragraph 15 above void or to annul it, on the basis that (a) it had not been duly published, (b) went beyond the statutory delegation and was too broad, and (c) contravened Article 8 of the Convention.

33. In June 2022 a three-judge panel of that court upheld the claim for judicial review, holding that the schedule, which it saw as a statutory instrument, had not been published, and that the procedure for its adoption had not been duly followed (*pew. № 6191 om 22.06.2022 г. no адм. д. № 12238/2021 г., BAC, VI о.*).

34. Following an appeal by the Agency, in December 2022 a five-judge panel of the same court quashed that judgment and remitted the case to another three-judge panel. It held that the initial three-judge panel had been incorrect to view the order as a statutory instrument; it was rather an internal act of the Agency, which meant that the rules governing the adoption and publication of statutory instruments did not apply to it (*печ. № 11947 от 21.12.2022 г. no адм. д. № 7413/2022 г., BAC, немчл. с-в*).

35. In January 2023 the new three-judge panel referred the case to the Sofia City Administrative Court, on the basis that that court (rather than the Supreme Administrative Court) had subject-matter jurisdiction to hear a claim directed against the schedule, which was an internal act of the Agency (*онп. № 544 от 17.01.2023 г. no адм. д. № 11878/2022 г., BAC, I o.*).

36. In June 2023 a three-judge panel of the Sofia City Administrative Court dismissed the claim, finding that the types of information set out in point 14 had been properly designated as “official secrets” (*печ. № 3623 от 02.06.2023 г. no адм. д. № 620/2023 г., АдмС-София-град*).

37. Mr Kanev appealed against that judgment, and in December 2023 the Supreme Administrative Court quashed it and remitted the case to the Sofia City Administrative Court, on the basis that under the rules of procedure it should have examined the claim in a single-judge formation rather than a three-judge panel (*печ. № 13059 от 28.12.2023 г. no адм. д. № 7313/2023 г., BAC, V o.*).

38. In March 2024 the Sofia City Administrative Court, sitting in a single-judge formation, dismissed the claim, giving the same reasons as earlier (*печ. № 1830 от 20.03.2024 г. no адм. д. № 90/2024 г., АдмС-София-град*).

39. Mr Kanev appealed to the Supreme Administrative Court. On 24 June 2025 that court dismissed the appeal, agreeing with the reasons given by the lower court (*печ. № 6883 от 24.06.2025 г. no адм. д. № 4426/2024 г., BAC, V o.*).

V. JUNE 2023 REQUEST TO THE AGENCY

A. The request and the Agency’s response to it

40. In mid-June 2023 Mr Kanev once again requested the Agency to inform him whether its databases contained information on whether he personally or the Committee (on whose behalf he was also acting) had been the target of intelligence-gathering, and whether during the previous ten years or earlier members or staff of the Committee had been recruited by the Agency.

41. At the end of June 2023 the Agency once again refused to disclose the information sought by Mr Kanev, again citing section 36(7) of the 2007 Act and the corresponding regulation (see paragraphs 69-70 below). It gave

almost the exact same reasons as those that it had given in July 2021 (see paragraphs 10-11 above), and added that under point 5 of part II of Schedule 1 to the Protection of Classified Information Act 2002 (see paragraphs 106 and 108 below), information that could lead to the identification of informers of the security services was a “State secret”.

B. Judicial review of the Agency’s refusal to disclose the information

1. Proceedings before the Sofia City Administrative Court

42. Mr Kanev, acting both in his personal capacity and on behalf of the Committee, sought judicial review under section 36(9) of the 2007 Act (see paragraph 72 below) of the new decision by the Agency to withhold the information that he was seeking.

43. In January 2024 the Sofia City Administrative Court set the Agency’s decision aside. It held that, in so far as Mr Kanev’s request had concerned other people (members or staff of the Committee), it had been irregular, as he had neither given the names of the people concerned nor produced authority to seek information on their behalf. A person could seek access only to his or her own personal data. By examining the request on the merits instead of referring it back to Mr Kanev for rectification, the Agency had breached the rules of procedure. The remainder of its decision had also been contrary to those rules, as the Agency had not set out the facts justifying its refusal to disclose information but had merely cited the relevant legal provisions. It had, moreover, disregarded its decision in respect of Mr Kanev’s June 2021 request (see paragraphs 9-11 above); that decision, which had become final after the unsuccessful legal challenge against it, would normally preclude a fresh decision on the same point. The matter was therefore to be referred back to the Agency with instructions to (a) direct Mr Kanev to rectify his request so far as it related to other people, (b) take into account its earlier decision, and (c) give proper reasons for its decision (*печ. № 136 от 05.01.2024 г. по адм. д. № 7471/2023 г., АдМС-София-град*).

2. Appeal proceedings before the Supreme Administrative Court

44. The Agency appealed against the Sofia City Administrative Court’s judgment.

45. In a final judgment of 16 July 2024 (*печ. № 8858 от 16.07.2024 г. по адм. д. № 2605/2024 г., БАС, V о.*), the Supreme Administrative Court partly upheld the lower court’s judgment.

46. It held that the lower court had been correct to find that, in so far as Mr Kanev’s request had concerned other people, it had been irregular, as Mr Kanev had neither given the names of those people nor produced evidence of his authority to seek information on their behalf. The lower court had also

been correct to find that the Agency had disregarded its final decision on the applicants' June 2021 request (see paragraphs 9-11 above).

47. The lower court had, however, erred by taking issue with the Agency's omission to set out the facts justifying its refusal to disclose information. The terms of section 36(8) of the 2007 Act (paragraph 71 below) made it clear that the Agency was under no duty to do so. It followed that the matter was indeed to be referred back to the Agency, but without instructions that it give any reasons on points of fact.

C. Renewed proceedings before the Agency

48. Having received the above-noted judgments, in early August 2024 the Agency invited Mr Kanev to rectify his request, in so far as it related to other people, by specifying the names of those people and by producing authority to seek information on their behalf.

49. In response, Mr Kanev urged the Agency to comply immediately with the judgments and to disclose whether its databases contained information that intelligence-gathering methods and techniques had been used with respect to him personally. As for his enquiry about intelligence-gathering activities targeting the Committee, he had neither asked the Agency to disclose information about other people, nor purported to act on behalf of other people; his request had concerned only information relating to the Committee itself. There was therefore nothing to rectify, and the Agency simply had to respond to the request and to disclose the requested information about the Committee.

50. In a decision of 22 August 2024 the Agency reiterated that it was barred by law from disclosing information to a person about other people, unless they had duly authorised the person seeking the information to do so on their behalf; it also pointed out that this had been confirmed by the courts that had reviewed its first response. Since Mr Kanev had not rectified that part of his request (the part relating to members or staff of the Committee), that request was to be viewed as irregular and not requiring examination. In so far as the request concerned Mr Kanev himself, it could not be examined with respect to the period preceding his earlier request (that made in June 2021 – see paragraph 8 above), since by law a public authority was precluded from re-examining a matter on which it had already decided with final effect, and in July 2021 the Agency had already made a decision (later upheld by the courts) in response to that earlier request (see paragraphs 9-11 and 12-27 above). As regards the period between June 2021 and June 2023, in relation to which there was no bar to the examination of the renewed request, the Agency refused the request, giving the same reasons, nearly word for word, that it had given in response to the June 2021 request (see paragraph 10 above). It also noted (as it had already done in June 2023 – see paragraph 41 above) that under point 5 of part II of Schedule 1 to the

Protection of Classified Information Act 2002 (see paragraphs 106 and 108 below), information that could lead to the identification of informers of the security services constituted a “State secret”.

51. Mr Kanev and the Committee have apparently not sought judicial review of that fresh decision by the Agency.

VI. INFORMATION REQUEST BY THE GOVERNMENT AGENT

52. In October 2023 the Government Agent in charge of the present case asked the Agency whether it had gathered data on the applicants. In its reply, dated 26 October 2023, the Agency stated that it had processed data of the applicants in connection with several access-to-information requests that they had made and related judicial review proceedings, including those in the present case. It could not, however, disclose whether someone had been of operational interest to it, since that kind of information – including information concerning the use of “special means of surveillance” – was classified, and its disclosure to the person concerned could compromise national security. That was why the legislature had only provided, in section 34g of the 1997 Act (see paragraph 82 (e) below), for the disclosure of information about the use of “special means of surveillance” with respect to someone if that use had been unlawful, rather than for a general possibility to check whether such means had been used with respect to that person. Information about informers of the Agency could not be disclosed either, for the reasons given in response to Mr Kanev’s requests (see paragraphs 11 and 41 *in fine* above).

RELEVANT LEGAL FRAMEWORK AND PRACTICE

I. BULGARIAN DOMESTIC LAW AND PRACTICE

A. State Agency for National Security Act 2007

1. The Agency, its tasks and powers

53. The State Agency for National Security Act 2007 (“the 2007 Act”) – which created the Agency and defined its tasks and powers – was enacted in December 2007 and came into force in January 2008.

54. The Agency is under the direct supervision of the government (section 2(1)). Its head is appointed by the President of the Republic, after being nominated by the government, and his or her two deputies are appointed by the government (section 8(1) and (2)). The Agency’s main tasks are to (a) safeguard national security from “encroachments directed against the national interests, independence and sovereignty of the Republic of Bulgaria, [its] territorial integrity, the fundamental rights and freedom of citizens, the democratic functioning of the State and the civic institutions, or the

established constitutional order” (section 4(1)), and (b) carry out counterintelligence – in particular, for the protection of strategic installations (section 4(2) and (4)). It may be given other tasks only by [means of] statute (section 7).

55. It has, for instance, been given various tasks in relation to:

(a) money laundering and the financing of terrorism (sections 4, 4a, 5, 5b, 9, 9a, 9b, 9v, 11, 11a, 13-14a and 15 of the Measures Against Terrorist Financing Act 2003, and sections 8, 9e, 36a, 68, 71-79, 81-85, 87-94, 103-04, 108-09 of the Measures Against Money Laundering Act 2018);

(b) combatting terrorism (sections 8(1) of the Terrorism Countermeasures Act 2016);

(c) the acquisition of Bulgarian nationality (sections 33 and 35 of the Bulgarian Citizenship Act 1998, and section 41(1)(3) of the 2007 Act);

(d) security vetting for clearance to access certain types of classified information (sections 11, 12, 14, 48-49 of the Protection of Classified Information Act 2002);

(e) migration control and the expulsion and related detention of aliens (sections 22(4), 24c(17), 24i(11), 24i(6), 33h(1), 33kk(8), 33p(9), 42g and 44 of the Aliens Act 1998, and section 41(1)(2) and (2) and (3) of the 2007 Act);

(f) the granting of asylum or humanitarian protection (section 58(10) of the Refugees and Asylum Act 2002, and section 41(1)(1) of the 2007 Act);

(g) the protection of nuclear installations (sections 112-14 of the Peaceful Use of Nuclear Energy Act 2002); and

(h) cybersecurity (section 15 of the Cybersecurity Act 2018).

56. In 2013-15 the Agency also had the task of investigating criminal offences related to national security (section 4(6) of the 2007 Act, added in June 2013 and repealed in February 2015).

57. The Agency’s two main areas of work are the gathering and analysis of intelligence (sections 18-20 and 28-29 of the 2007 Act). It can, in particular, engage in information analysis, forecasting and control (*прогностична [и] контролна дейност*), using its own information or information obtained from other authorities that is of importance for national security (section 4(3)). It may monitor people, objects and activities (section 5).

58. The Agency may (a) check databases in relation to people engaging in offences endangering national security; (b) carry out surveillance; (c) enter and search premises, buildings, installations, vehicles or locations; (d) intercept telephone conversations; (e) obtain information from other communication channels; and (f) use not-for-profit legal persons or commercial companies (section 20(1)(2), (1)(6), (1)(8)-(1)(11) and (1)(20) of the 2007 Act). It can do all that through “specific methods and techniques”, “special means of surveillance”, and people collaborating with it (section 20(2)).

59. Section 21 of the 2007 Act specifies that the Agency has at its disposal and may deploy “special means of surveillance”, under the conditions laid down in the 1997 Act (see paragraph 82 below).

60. The Agency may maintain and use databases (section 28(1) of the 2007 Act) and process information – including personal data (section 29(1) and (2)).

2. Informers recruited by the Agency

61. The Agency may use informers (*сътрудници*), who must be protected in the course of or in connection with their collaboration (section 23(1) and (3)(2) of the 2007 Act). Their identities, personal data and work must be kept secret (section 23(3)(3)). Information about them may only be passed to the courts or the prosecuting authorities in connection with a specific criminal case, in keeping with the requirements of the Protection of Classified Information Act 2002 (see paragraphs 106-111 below) – and only after the informers in question have agreed to that (section 23(4)). The Agency may also withhold information about informers to protect its intelligence-gathering methods or techniques (section 35a).

3. Personal data processed by the Agency

62. The Agency’s databases may be automated (sections 34(1) and 36(2) of the 2007 Act). They may be used to process personal data (section 34(2)). The data controller is the head of the Agency, who may entrust the processing to designated officials (section 34(9)).

63. When processing personal data relating to any activities related to safeguarding national security, the Agency does not (a) seek the consent of the people concerned; (b) inform them before or during the processing; or (c) make available the personal data of other people (section 34(2)). Those personal data are to be deleted if there is no longer any lawful reason for keeping them or if so ordered by a court (section 34(5)). The factors to be taken into account in that assessment comprise: the age of the individual concerned, the nature of the data being processed, the need to process them until the conclusion of a legal procedure or investigation, and the expiry of any statutory limitation period (section 34(6)). Personal data from the Agency’s databases may be given only to the authorities safeguarding national security or the judicial authorities for the needs of a specific criminal case (section 34(7)). Those data may also be given to foreign authorities pursuant to an international treaty to which Bulgaria is party (section 34(8)).

64. The Agency may not gather information about: political, religious or philosophical convictions: the membership of any political parties or organisations, the membership of associations that have religious, philosophical, political or trade-union aims; or someone’s health or sexuality (section 35(1)).

65. Regulations issued by the head of the Agency in October 2019 pursuant to a statutory delegation in section 34(10) of the 2007 Act (*Наредба № I-4 от 22.10.2019 г. за реда за обработване на лични данни в Държавна агенция „Национална сигурност“*) lay down more detailed rules on the processing of personal data by the Agency. By regulation 2, that processing must be consistent with the principles of lawfulness, integrity, relevance and proportionality, and data security. By regulation 4, the head of the Agency: (a) fixes how the Agency creates, runs and controls databases containing personal data; (b) checks whether the processing of such data meets the requirements for its protection; (c) takes steps to rectify irregularities; and (d) assists the Commission for the Protection of Personal Data (see paragraphs 97-101 below) in the exercise of its supervisory functions under the Protection of Personal Data Act 2002 (see paragraphs 84-105 below). The head of the Agency (a) determines which Agency officers may process personal data (regulation 6(1)), and (b) decides, in each individual case, whether such data processed by the Agency is to be deleted, on the basis of a recommendation by the respective head of unit (regulation 17).

(a) Access to personal data processed by the Agency

(i) Relevant statutory provisions and regulations

66. Agency officers may not disclose information held by the Agency to other State authorities, organisations, legal persons or private persons, except as prescribed by law (section 35(3) of the 2007 Act).

67. Anyone is entitled to request access to personal data that relate to him or her and are being processed in the Agency's databases without his or her knowledge (section 36(4)). The head of the Agency or a duly authorised deputy must respond to such a request within fourteen days of its being made (section 36(5)). If an individual asks, he or she must be given a paper copy of any personal data relating to him or her that is being processed by the Agency (section 36(6)).

68. If the exercise of the right of access could reveal someone else's personal data, the data controller must give access only to those data that concern the individual requesting access (section 35(2)).

69. The exact manner of accessing the Agency's databases is prescribed in regulations made by its head (section 36(10)). Those regulations (*Наредба № I-7 от 13.07.2009 г. за реда за достъп до информационните фондове на Държавна агенция „Национална сигурност“*) were issued in 2009 and prescribe, among other things, that if a person lodges an incomplete access request, the Agency must advise him or her of that; and if that person then fails to rectify the request, it is not examined (regulation 7(1) and (2)).

70. The Agency may refuse, wholly or in part, to disclose data if doing so would endanger national security, the protection of information classified as

constituting a “State secret” or an “official secret” (for the definitions of the two terms in Bulgarian law, see paragraphs 107-109 below), or the confidentiality of its sources of information or the covert methods and techniques that it uses to gather that information, or if disclosure would otherwise hinder the Agency’s statutory tasks (section 36(7) and regulation 11(1)).

71. A person whose request has been refused must be advised of that in writing, but only the legal grounds for that refusal need to be given (section 36(8) and regulation 11(2)). The absence of a response within the time-limit is deemed to constitute a refusal (section 36(8) *in fine*).

72. Any such refusal is open to legal challenge under the relevant provisions of the Code of Administrative Procedure (section 36(9)) – in particular, by way of judicial review.

(ii) *Case-law of the Bulgarian courts under those provisions*

(α) 2012 case

73. In a 2012 judgment (*peu. № 593 om 08.02.2012 г. no адм. д. № 6653/2011 г., АдмС-София-град*) – which was apparently not appealed against – the Sofia City Administrative Court dismissed a claim for judicial review by a non-governmental organisation in respect of a refusal by the Agency to disclose how many such organisations it had investigated between January 2008 and July 2011, and what results any such enquiries had yielded. The court found, among other things, that information about the operations of the security services and their results was a “State secret”, and on that basis held that the information sought by the organisation was classified. It went on to state that the disclosure of such information was also proscribed by section 36(7) of the 2007 Act (see paragraph 70 above).

(β) 2014-18 case

74. In a 2014 judgment (*peu. № 13080 om 04.11.2014 г. no адм. д. № 6237/2014 г., BAC, V o.*), the Supreme Administrative Court set aside the tacit refusal of the Agency to disclose whether it was processing a certain person’s data, and, if so, to give that person’s access to any data pertaining to him that it was processing. The court held that in the absence of an express decision taken by the Agency, there was no material indicating that any information regarding the data of the person in question had properly been withheld. It had to be ascertained in all such cases that the Agency, as a data controller, had duly assessed, with reference to the relevant rules (including section 36(7) – see paragraph 70 above), that the information in question ought not to be disclosed.

75. Following that judgment, the Agency expressly stated its refusal to disclose such information, stating that to do so would expose its sources and methods. The Varna Administrative Court dismissed the claim for judicial

review of that decision, and in 2018 the Supreme Administrative Court upheld its judgment. It cited section 36(7) (see paragraph 70 above), and briefly noted that by section 3(1) of the Protection of Classified Information Act 2002 (see paragraph 112 *in fine* below), only people with security clearance who needed such classified information for their specific tasks could access it (see *peu. № 94 om 04.01.2018 г. no адм. д. № 5244/2016 г., BAC, V o.*).

(γ) 2021-22 case

76. In a July 2021 judgment (*peu. № 4760 om 16.07.2021 г. no адм. д. № 3553/2021 г., АдмС-София-град*), the Sofia City Administrative Court dismissed a claim for judicial review of a refusal by the Agency to disclose whether it was processing a person's data, and, if so, to afford her access to any of her personal data that it might be processing. The court gave nearly the same reasons as those it gave four months later, in November 2021, for dismissing the applicants' first claim for judicial review in the present case (see paragraph 19 above). An appeal against its judgment was dismissed on procedural grounds, without reference to the merits, because it was defective and the claimant failed to rectify it within the time directed by the court (see *onp. № 3358 om 08.04.2022 г. no адм. д. № 798/2022 г., BAC, V o.*).

(b) Supervision of the processing of personal data by the Agency

77. Section 37 of the 2007 Act, as originally enacted (and not amended since) provides that supervision of the protection of the rights of individuals in the course of the processing of their personal data by the Agency and of access to those data should be carried out by the Commission for the Protection of Personal Data, under the conditions and in the manner laid down by the Protection of Personal Data Act 2002 (see paragraphs 84-101 below).

4. General supervision of the Agency's work

(a) By Parliament

78. The Bulgarian Parliament (the National Assembly) has a special standing committee – the Committee for the Oversight of the Security Services, of the Application and Use of Special Means of Surveillance, and of Access to the Data under the Electronic Communications Act – which is tasked with, among other things, supervising the work of the Agency under: section 132(1) of the 2007 Act and section 22(1) of the Management and Functioning of the System for Protecting National Security Act 2015 (“the 2015 Act”); Rule 16 § 1 (11) of the 2021-22, 2022-23 and 2023-24 Rules of the National Assembly (which has been superseded by Rule 16 § 1 (10) of the 2024 Rules of the National Assembly); and Rule 4 of the latest (and nearly identical) iterations of the Committee's Rules, which were adopted in January 2022, November 2022, May 2023 and July 2024).

In 2021-23 the Committee had fourteen members, and has since May 2023 had twelve members. The Committee is reconstituted by each new Parliament. According to all of the successive decisions for its election (the latest ones were taken in December 2021, October 2022, May 2023 and July 2024), it must comprise members of Parliament from each parliamentary group. It must scrutinise, in particular, whether in their work the security services comply with the legal provisions guaranteeing basic human rights (Rule 15 § 1 (6) of the Committee's Rules). It can ask the security services to produce thematic reports (Rule 15 § 1 (4) of the Committee's Rules). It can also examine reports by individuals or organisations about misconduct by officers of the security services (Rule 15 § 1 (9) of the Committee's Rules), and refer unlawful conduct by those services that it has spotted in the course of its own inspections (or which have been complained of by individuals) to the prosecuting authorities or other competent authorities (Rule 15 § 1 (10) of the Committee's Rules).

79. The Agency's head, deputy heads and officers must appear before Parliament or the Committee if they are invited to do so, and make available to them any information that they are required to disclose (section 132(2) of the 2007 Act, section 22(2) of the 2015 Act, and Rule 15 § 1 (5) of the Committee's Rules). Section 22(2) *in fine* of the 2015 Act goes on to prescribe that this must be done in a manner that is consistent with the requirements of the Protection of Classified Information Act 2002.

(b) By the Government

80. The head of the Agency presents to the government an annual report about the Agency's work, and the government then submits that report to the Parliament, which approves it (section 132(3) of the 2007 Act, and section 22(3) of the 2015 Act).

(c) By the President of the Republic

81. The President of the Republic may require the head of the Agency to produce analyses of questions relating to national security (section 132a of the 2007 Act).

B. Special Surveillance Means Act 1997

82. The Special Surveillance Means Act 1997, as amended ("the 1997 Act"), and its application were recently described in detail in *Ekimdzhiev and Others* (cited above, §§ 11-135). In the present case, it merely needs to be noted that:

(a) the only authorities that may seek the use of "special means of surveillance" outside the framework of already pending criminal proceedings are: (i) the various directorates of the Ministry of Internal Affairs; (ii) the Agency's territorial directorates and units; (iii) the military intelligence and

military police services under the control of the Minister of Defence; (iv) the Intelligence Agency; (v) regional prosecutor's offices (only in relation to serious electoral offences); and (vi) the specialised anti-corruption directorate (section 13(1) of the 1997 Act). In criminal proceedings, that may be done by the public prosecutor in charge of supervising the pre-trial investigation (section 13(2) of the 1997 Act and Article 173 § 1 of the Code of Criminal Procedure);

(b) as a rule, surveillance warrants may be issued only by the presidents of the Sofia City Court, of the respective regional or military courts (and, between August 2011 and July 2022, the now defunct Specialised Criminal Court), or an expressly authorised deputy (section 15(1) and (2) of the 1997 Act and Article 174 §§ 1-2 of the Code of Criminal Procedure);

(c) the only authorities that may deploy "special means of surveillance" are (i) the Technical Operations Agency under the direct supervision of the government; (ii) the Agency's Technical Operations Directorate; (iii) the State Intelligence Agency (within its particular sphere of authority); (iv) the intelligence services of the Ministry of Defence (also within their particular sphere of authority); and (v) (but only as regards undercover agents, controlled deliveries and pseudo-transactions¹) the Ministry of Internal Affairs (section 20(1) and (2) of the 1997 Act);

(d) general supervision of the use of "special means of surveillance" has since 2013 been entrusted to the National Bureau (see paragraph 5 above, and *Ekimdzhiev and Others*, cited above, §§ 108-24); and

(e) the National Bureau must notify people placed under covert surveillance only if that surveillance was unlawful, and only if such notification would not (i) defeat the purpose of the surveillance, (ii) reveal the techniques or equipment used to carry it out, or (iii) entail a risk to the life of an undercover agent or his or her relatives or friends (section 34g of the 1997 Act). In two decisions delivered in 2016, the Supreme Administrative Court held that such notifications by the Bureau could not be subject to judicial review (see *Ekimdzhiev and Others*, cited above, § 133).

83. The National Bureau's annual reports for 2022 and 2023 recorded that the Agency's respective share of all applications for warrants for "special means of surveillance" had been, respectively, 11.27% of the total number of such applications made in 2022 and 10.88% of the total number of such applications made in 2023.

C. Protection of Personal Data Act 2002

84. The Protection of Personal Data Act 2002 ("the 2002 Act") was enacted to, among other things, ensure that Bulgaria would comply with its obligation under the 1981 Convention for the Protection of Individuals with

¹ Those also sometimes described as "simulated purchases" or "test purchases".

regard to Automatic Processing of Personal Data, which it had signed in 1998 and ratified in 2002 (see paragraph 179 below), to take the necessary measures in its domestic law to give effect to the basic data-protection principles.

85. As amended with effect from March 2019 with a view to (a) being brought into line with the GDPR (see paragraph 132 below), and (b) transposing Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data (“Law Enforcement Directive” – “the LED” – see paragraph 149 below), the 2002 Act regulates all matters relating to the protection of personal data that are not set out in the GDPR itself (section 1(1)).

86. By paragraph 1(1) of the 2002 Act’s additional provisions (as amended with effect from March 2019), “personal data” for the purposes of the Act has the meaning given to the term in Article 4 (1) of the GDPR (see paragraph 133 below).

1. Scope of application

(a) *Ratione personae*

87. The provisions of the 2002 Act, irrespective of whether they concern the processing of personal data falling within the scope of the GDPR or the processing of such data by the authorities for law-enforcement purposes, apply only to data relating to individuals (that is, natural persons) (section 1(1) and (2)).

(b) Application to processing for national security purposes

88. The 2002 Act, as worded since March 2019, does not apply to the processing of personal data for national security purposes, unless that is expressly provided for elsewhere (section 1(5)). The explanatory notes to the government bill (no. 802-01-27) which led to the March 2019 amendments to the Act (see paragraph 84 above) stated that section 1(5) had been put in place to reflect the position that the GDPR and the LED did not apply to the processing of personal data for activities falling outside the scope of European Union (EU) law (see paragraphs 123, 134-136 and 151-152 below). In a November 2023 judgment (*peu. № 10522 om 02.11.2023 г. no адм. д. № 140/2023 г., BAC, V о.*), the Supreme Administrative Court pointed out that national security purposes within the meaning of section 1(5) were to be distinguished from law-enforcement purposes.

89. When originally enacted, the 2002 Act stated that the processing of personal data for national security purposes could be governed by a special statute (section 1(4), as worded in 2002-05). In 2005 that subsection was

amended to provide that such processing was to be governed by a special statute (section 1(4), as worded in 2005-06). In late 2006 section 1(4), which became section 1(5), was amended once more – this time to state that the Act did apply to the processing of personal data for national security purposes unless a special statute provided otherwise (section 1(5), as worded in 2006-19).

90. During that period, in 2014, the authority in charge of supervising the application of the 2002 Act, the Commission for the Protection of Personal Data (see paragraph 97 below), received a complaint by an individual suspecting that the Agency had covertly intercepted his telephone communications. He had asked the Agency for information on the point under the 2002 Act, and the Agency had refused to give it, stating that it fell outside the scope of that Act. He then complained of that refusal to that Commission, which dismissed his complaint, agreeing that the information which he had sought from the Agency fell outside the scope of the 2002 Act as it did not concern personal data. According to that Commission, information about the use of “special means of surveillance” could be sought only from the National Bureau (see paragraph 82 (e) above) (see *peu. № Ж-780 om 08.10.2014 г., КЗЛД*).

2. Right to access personal data and restrictions on that right

(a) In relation to processing falling within the scope of the GDPR

91. The right of access to information whose processing falls within the scope of the GDPR is governed by its Article 15(1)(a) (see paragraph 137 below).

92. A data controller or processor may restrict, wholly or in part, the data subject’s access or other rights under Articles 12-22 of the GDPR if their exercise would create a risk for national security (section 37a(1)(1) of the 2002 Act, which reflects Article 23(1)(a) of the GDPR – see paragraph 138 below). Section 37a(2) specifies that the way in which this can be done must be prescribed by law and consistent with Article 23(2) of the GDPR.

(b) In relation to processing by the authorities for law-enforcement purposes

93. A data subject is entitled to obtain from the controller confirmation of whether personal data concerning him or her are being processed, and (if they are) access to those data and to information about the purposes of their processing (section 55(1)(1) read in conjunction with section 54(1)(5) and (2)(1) of the 2002 Act, which transposed Article 14 (a) of the LED – see paragraph 153 below).

94. Those rights may be restricted wholly or in part if that is necessary to, among other things, safeguard national security – so long as due regard is paid to the fundamental rights and legitimate interests of the persons concerned (section 55(3) read in conjunction with section 54(3)(4) of the

2002 Act, which implemented the exemption permitted by Article 15(1)(d) of the LED – see paragraph 156 below). When the obstacle ceases to exist, the data controller must normally provide that information within two months of it being requested by the data subject (section 55(3) *in fine* read in conjunction with sections 54(4) and 53(3)).

95. If access to personal data is refused or restricted under the above-noted provisions, the data controller must inform the data subject of that refusal or the restriction (and of the reasons therefor) within two months, but may omit to do so if that would defeat the purpose of those measures (section 55(4) read in conjunction with section 53(3) of the 2002 Act, which transposed Article 15(3) of the LED – see paragraph 158 below). In that event, the data controller must nonetheless record the factual and legal reasons on which that decision rests, and make them available to the competent supervisory authority – which is, in most cases, the Commission for the Protection of Personal Data, whose tasks and powers are set out in paragraphs 97-101 below (section 55(5) of the 2002 Act, which transposed Article 15(4) of the LED – see paragraph 159 below).

96. If such restrictions have been put in place by a data controller that is not a court or a prosecuting or investigating authority,² the data subject may exercise his or her right of access under section 55(1) of the 2002 Act indirectly, through the Commission for the Protection of Personal Data. If the data subject does so, that Commission must check the lawfulness of the restriction (section 57(1) of the 2002 Act, which transposed Article 17(1) of the LED – see paragraph 162 below), and inform the data subject at least that all necessary verifications or a review have taken place (section 57(2) of the 2002 Act, which transposed Article 17(3) of the LED – see paragraph 163 below).

3. *Supervisory authority*

97. The Commission for the Protection of Personal Data supervises the processing of personal data falling within the scope of the GDPR, as well as such processing for law-enforcement purposes by all authorities, except the courts and the prosecuting and investigating authorities (sections 6(1), 10(1), 10a(1) and 78 of the 2002 Act).³

98. In carrying out that supervision, that Commission must, among other things, (a) handle complaints by data subjects, (b) check the lawfulness of the processing in cases in which the data subject's access right has been restricted (see paragraphs 94 and 96 above), and (c) inform the data subject within three

² The processing of personal data for law-enforcement purposes by the courts and by the prosecuting and investigating authorities (which by Article 117 § 2 of the 1991 Constitution of Bulgaria are also part of the judicial branch) is supervised by the Supreme Judicial Council's Inspectorate (section 78(2) of the 2002 Act).

³ See footnote 2 above.

months of the outcome of that verification or of the reasons for it not being carried out (Article 57 § 1 (f) of the GDPR and section 79(1)(5) and (1)(6) of the 2002 Act, which transposed Article 46(1)(f) and (g) of the LED – see paragraph 170 below).

99. When supervising data processing for law-enforcement purposes, that Commission may obtain from the controller or the processor access to (a) all personal data being processed and (b) all the information necessary for it to carry out its tasks (section 80(1)(1) and (1)(2) of the 2002 Act, which transposed Article 47(1) of the LED – see paragraph 171 below).

100. When supervising data processing for law-enforcement purposes, that Commission may (a) order the controller or processor to bring processing operations into compliance with the relevant part of the 2002 Act – in particular, by ordering the rectification or erasure of personal data or the restriction of their processing, pursuant to section 56 of the Act, and (b) impose a temporary or definitive limitation, including a ban, on processing (section 80(1)(3) and (1)(4)) of the 2002 Act, which transposed Article 47(2)(b) and (c) of the LED). The Commission has exercised those powers on at least three occasions with respect to the Ministry of Internal Affairs (see *peu. № IIIH-01-482/2020 om 10.05.2021 г., K3/JI*; *peu. № IIIH-01-361/2021 om 18.01.2022 г., K3/JI*; and *peu. № IIIH-01-350/2021 г. om 17.03.2022 г., K3/JI*).

101. That Commission may also bring infringements of the relevant part of the 2002 Act to the attention of the courts (section 80(3) of the 2002 Act, which transposed Article 47(5) of the LED – see paragraph 173 below).

102. In its annual report for 2009, that Commission recorded, on page 28, that it had entered into a cooperation agreement with the Agency for the purpose of realising closer collaboration between the two in the area of personal-data protection (in a spirit of respect for each other's independence and respective areas of responsibility); that cooperation encompassed the coordination, exchange, holding and use of data and information, as well as the creation of joint working groups and the provision of expert or technical assistance. The Commission also noted, on page 35 *in fine*, that it was about to finalise an audit of the Agency in connection with preparations for the future implementation of the Schengen Information System. In its annual report for 2010, the Commission recorded, on page 38, that it had continued its cooperation with the Agency pursuant to the agreement made in 2009. In its annual report for 2015, the Commission referred, on pages 42-43, to a check on a private foundation that it had carried out together with other authorities, including the Agency. In its annual report for 2016, the Commission referred, on pages 98-99, to its cooperation with the Agency regarding the transposition of new legislation (for instance, regarding the creation of a new financial-intelligence unit within the Agency) and international cooperation. The Commission has not mentioned, in any of its annual reports for the period 2009-23, any inspections which it has carried

out in the Agency apart from the above-mentioned 2009 audit relating to the future implementation of the Schengen Information System.

4. Remedies

(a) In respect of processing falling within the scope of the GDPR

103. Data subjects considering that their rights under the GDPR or the 2002 Act have been breached may complain to the Commission for the Protection of Personal Data, and seek judicial review of its decision (section 38(1) and (7) (since May 2023 subsection (8)) of the 2002 Act, which reflects Articles 77(1) and 78(1) and (2) of the GDPR – see paragraphs 145 and 147 below).

104. Data subjects may also directly seek judicial review of actions undertaken or decisions issued by the data controller or processor, or damages from them, if the data controller or processor have processed their personal data unlawfully (section 39(1) and (2) of the 2002 Act, which reflects Articles 79(1) and 82(1) of the GDPR – see paragraphs 146 and 148 below).

(b) In respect of processing undertaken by the authorities for law-enforcement purposes

105. The remedies for alleged breaches of the rights of data subjects that occur in the course of the processing of personal data by the authorities for law-enforcement purposes are the same as those for alleged breaches in the course of processing that fall within the scope of the GDPR (section 82(1) of the 2002 Act, which transposed Articles 52(1), 53 and 54 of the LED – see paragraphs 174-178 below).

D. Protection of Classified Information Act 2002

1. Types of classified information

106. By section 1(3) of Protection of Classified Information Act 2002, classified information comprises (a) "State secrets", (b) "official secrets", and (c) classified information obtained from another State.

107. Section 25 defines a "State secret" as "information [covered by] Schedule 1 [to the Act], unregulated access to which could endanger or harm the interests of the Republic of Bulgaria and which relates to national security, defence, foreign policy, or the protection of constitutional order". Schedule 1 sets out the categories of information liable to be classified as being a "State secret". Under point 5 of part II of that Schedule, that includes information which could lead to the identification of informers of the security services.

108. Section 26(1) defines an "official secret" as "information created or stored by State or local authorities which is not a State secret, but to which unregulated access could negatively affect the interests of the State or another interest protected by law". Paragraph 1(3) of the additional provisions of

the 2007 Act (see paragraph 53 above) contains a similar definition; however, it refers to “information relating to the Agency’s functions and tasks, or the exercise of its powers, or [information] resulting from that” and specifically to a possible negative effect on “the activities of the Agency [and] its staff in respect of the performance of their duties, or [on] third persons”.

109. The types of information liable to be classified as an “official secret” are to be prescribed by statute (section 26(2)). The head of the respective authority must then, within those bounds, set the categories of information falling within the authority’s sphere of operation that are to be so classified (section 26(3)). As regards, in particular, the Agency, the categories of information that are processed by it and that are to be classified as an “official secret” are to be specified in an order issued by its head (section 32 of the 2007 Act); such an order was issued in May 2020 (see paragraph 15 above).

2. Time-limits for protecting classified information

110. Section 28 of the Act sets out the levels of classification. Information that is a “State secret” is to be marked as “top secret”, “secret” or “confidential”, depending on the degree of harm that its unauthorised disclosure could entail. Information that is an “official secret” is marked “for official use only”.

111. Section 34(1) lays down the time-limits for protecting classified information: thirty years if it is “top secret”; fifteen years if it “secret”; five years if it is “confidential”; and six months if it is graded as an “official secret”. These time-limits may be extended only once – for up to twice their original length (section 34(2)).

3. Access to classified information by lawyers and litigants

(a) Relevant provisions of the Act

112. The general rule under the Act is that no person may have access to classified information belonging to one of the top three categories of classification (see paragraph 106 above) unless that is necessary for the performance of their professional duties or tasks (“need to know”), and unless he or she has been given clearance after a security screening (section 3(1) and (2) and section 38(1)(1)).

113. Section 39 details the cases in which such screening is not required. That is generally the case for people holding certain high-ranking posts. In contrast to other officials, people holding certain particularly high-ranking posts (Speaker of Parliament, President of the Republic and Prime Minister) are not constrained by the “need-to-know” limitation and are *ex officio* entitled to access any classified information (section 39(1) and (2)). Others, such as government ministers and members of Parliament, have automatic access to classified information coming within their sphere of responsibility, on a “need to know” basis (section 39(1) and (3)).

114. Constitutional Court judges, judges, prosecutors and investigators are likewise entitled to access, without undergoing security screening, all levels of classified information relating to cases that they are dealing with, again on a “need to know” basis (section 39(1) and (3)(3)). A June 2004 amendment to section 39(3)(3) extended this category to include practising lawyers.

115. A new section 39a, added in October 2004, provides, in subsection 1, that persons who need to access classified information in the course of or in connection with the exercise of their “constitutional right to defence” do not need to undergo security screening. Subsection 2 goes on to prescribe that such persons are entitled to access to all levels of classified information for the duration necessary to exercise their “right to defence”, on a “need to know” basis.

116. The specific wording of that new section 39a was not in the original government bill (no. 402-01-41) which led to its enactment. The wording emerged in the course of deliberations on that bill in Parliament’s Legal Affairs Committee on 29 September 2004, between its first and second plenary reading, and was based on a proposal by two representatives of the State Commission on the Security of Information – the body overseeing the storage and use of classified information – who were also present at the deliberations. In the course of the discussion on the exact wording of the provision, a member of the Committee opined that it would concern access to classified information already available in the case file of the relevant case. At the second plenary reading of the bill on 30 September 2004, the new section 39a, as proposed by that Committee, was adopted by Parliament without any discussion, by 91 votes to nil.

(b) Case-law and practice of the administrative courts under sections 39(3)(3) and 39a of the Protection of Classified Information Act 2002

117. The reported cases dealing with the application of sections 39(3)(3) and 39a of the Act (see paragraphs 114 *in fine* and 115 above) by the administrative courts are few.

118. In seven cases which it examined in 2019-23 and which concerned (a) a disciplinary sanction imposed on an employee of the Agency, and (b) several decisions of the Agency in relation to an employee whom it had dismissed (refusals to reinstate him, or reinstate him as expected by him, his temporary removal from duty, his follow-up dismissal, and so on), the Pleven Administrative Court indicated to the judicial review claimants that they, respectively their lawyers, were entitled, under section 39a, respectively section 39(3)(3), to access the classified information in the cases produced by the Agency (see *onp. № 2080 om 18.10.2019 г. no адм. д. № 1031/2019 г., АдмС-Плевен; onp. № 1379 om 17.09.2020 г. no адм. д. № 492/2020 г., АдмС-Плевен; onp. № 1387 om 18.09.2020 г. no адм. д. № 315/2020 г., АдмС-Плевен; onp. № 109 om 21.01.2022 г. no адм. д. № 934/2021 г.,*

АдмС-Плевен; опр. № 961 от 18.05.2022 г. по адм. д. № 349/2022 г., АдмС-Плевен; опр. № 1665 от 23.08.2022 г. по адм. д. № 102/2022 г., АдмС-Плевен; and опр. № 346 от 13.02.2023 г. по адм. д. № 90/2023 г., АдмС-Плевен).

119. In 2012 and 2024 respectively, in a case relating to the expropriation of a property and a case relating to a refusal to grant international protection, the Sofia City Administrative Court likewise held that section 39a gave the judicial review claimants the right to access classified information (see *реш. № 1565 от 23.03.2012 г. по адм. д. № 5906/2011 г., АдмС-София-град*, and *опр. № 2119 от 06.11.2024 г. област по адм. д. № 1222/2024 г., АдмС-София*).

120. By contrast, in three other cases, which it decided in 2016, 2021 and 2022, the Sofia City Administrative Court held that section 39a applied only if the litigants were facing criminal or disciplinary charges (see *реш. № 6140 от 10.10.2016 г. по адм. д. № 5115/2016 г., АдмС-София-град*; *реш. № 2650 от 20.04.2021 г. по адм. д. № 703/2021 г., АдмС-София-град*; and *реш. № 3750 от 07.06.2022 г. по адм. д. № 4518/2022 г., АдмС-София-град*). Likewise, in two cases relating to the detention of asylum-seekers which it decided in 2002 and 2023, that court held – in response to submissions by counsel for the claimants that pursuant to section 39a they had to be given access to classified information produced by the Agency – that the absence of access to that information had not been a breach of the rules of procedure because it was classified (see *реш. № 8007 от 23.12.2022 г. по адм. д. № 9515/2022 г., АдмС-София-град*, and *реш. № 1653 от 15.03.2023 г. по адм. д. № 11213/2022 г., АдмС-София-град*).

121. In two judgments given in 2018 and relating to refusals to grant aliens international protection, the Supreme Administrative Court held that under section 39a, respectively section 39(3)(3), the claimants, respectively their lawyers, had been entitled to access the classified information produced by the Agency in support of its assertion that they presented a national security risk, so as to be able to pursue effectively their legal challenges against the refusals to grant them international protection (see *реш. № 8286 от 19.06.2018 г. по адм. д. № 1782/2018 г., ВАС, III о.*, and *реш. № 10759 от 04.09.2018 г. по адм. д. № 4056/2017 г., ВАС, III о.*).

E. Management and Functioning of the System for Safeguarding National Security Act 2015

122. Section 2 of the Management and Functioning of the System for Safeguarding National Security Act 2015 defines “national security” as “a dynamic state of society and the State in which the territorial integrity, sovereignty and constitutional order are protected, and the democratic functioning of the institutions and the fundamental rights and freedoms of

citizens are guaranteed, as a result of which the nation preserves and increases its welfare and develops, and the country successfully protects its national interests and realises its national priorities”.

II. EUROPEAN UNION (EU) LAW

A. Treaty on European Union

123. By Article 4(2) of the Treaty on European Union (OJ 2016/C 202/01, p. 13 – “TEU”), national security “remains the sole responsibility” of each EU member State.

B. Treaty on the Functioning of the European Union

124. By Article 16(1) of the Treaty on the Functioning of the European Union (OJ 2016/C 202/01, p. 47 – “TFEU”), “[e]veryone has the right to the protection of personal data concerning them”.

125. Article 16(2) of the TFEU mandated the European Parliament and the European Council to lay down rules relating to the protection of individuals with regard to the processing of personal data by EU institutions, bodies, offices and agencies, and by EU member States when carrying out activities which fall within the scope of EU law, and the rules relating to the free movement of such data”, adding that compliance with these rules is to be subject to the control of independent authorities.

126. By Article 16(3) of the TFEU, read in conjunction with Article 39 of the TEU, the rules adopted on the basis of Article 16(2) are to be without prejudice to the rules (to be laid down in a decision of the European Council under Article 39 of the TEU) relating to the protection of individuals with regard to the processing of personal data by EU member States when carrying out activities falling within the scope of the EU’s common foreign and security policy.

C. Charter of Fundamental Rights of the European Union

127. By Article 7 of the of the Charter of Fundamental Rights of the European Union (OJ 2016/C 202/02, p. 389 – “the Charter”), entitled “Respect for private and family life”, “[e]veryone has the right to respect for his or her private and family life, home and communications”.

128. Article 8 of the Charter, entitled “Protection of personal data”, reads:

“1. Everyone has the right to the protection of personal data concerning him or her.

2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which have been collected concerning him or her, and the right to have them rectified.

3. Compliance with these rules shall be subject to control by an independent authority.”

129. By Article 47 of the Charter, entitled “Right to an effective remedy and to a fair trial”, “[e]veryone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article”.

130. By Article 51 of the Charter, entitled “Scope”, its provisions are addressed to EU member States only when they are implementing EU law.

131. Article 52 of the Charter, entitled “Scope of guaranteed rights”, reads, in so far as relevant:

1. Any limitation on the exercise of the rights and freedoms recognised by this Charter must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

...

3. In so far as this Charter contains rights which correspond to rights guaranteed by the Convention for the Protection of Human Rights and Fundamental Freedoms, the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection.”

D. General Data Protection Regulation

132. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (OJ 2016 L 119, p. 1) (“General Data Protection Regulation” – “the GDPR”) entered into force in 2016 but applies from 25 May 2018 (Article 99(2)).⁴ It applies to “natural persons”, and does not cover the processing of personal data that concern legal persons (recital 14).

133. Article 4(1) of the GDPR defines “personal data” as “any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person”.

⁴ Article 94(1) of the GDPR repealed Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ 1995 L 281, p. 31 – “Data Protection Directive”) with effect from 25 May 2018.

1. *Scope of application ratione materiae*

134. Article 2(2)(a) of the GDPR states that it “does not apply to the processing of personal data ... in the course of an activity that falls outside the scope of [EU] law”. The related recital 16 states that the GDPR “does not apply to issues of protection of fundamental rights and freedoms or the free flow of personal data related to activities which fall outside the scope of [EU] law, such as activities concerning national security”.

135. The Court of Justice of the European Union (“CJEU”) has held that the activities aimed at safeguarding national security set out in Article 2(2)(a) of the GDPR “encompass, in particular, those that are intended to protect essential State functions and the fundamental interests of society” (see judgments of the CJEU of 22 June 2021 in *Latvijas Republikas Saeima (Penalty points)*, C-439/19, EU:C:2021:504, paragraph 67; of 20 October 2022 in *Koalitsia ‘Demokraticzna Bulgaria – Obedinenie’*, C-306/21, EU:C:2022:813, paragraph 40; and of 5 June 2023 in *Commission v. Poland (Independence and private life of judges)*, C-204/21, EU:C:2023:334, paragraph 318).

136. On that basis, the CJEU recently found that the activities of a parliamentary committee investigating the operations of a State-protection authority (prompted by suspicions of political influence being exercised over that authority) could not be viewed as activities concerning national security falling outside the scope of EU law within the meaning of Article 2(2)(a) of the GDPR (see judgment of the CJEU of 16 January 2024 in *Österreichische Datenschutzbehörde*, C-33/22, EU:C:2024:46, paragraph 57).

2. *Right to access personal data*

137. A data subject is entitled to obtain from the controller confirmation of whether personal data concerning him or her are being processed, and, if that is so, access to those data and information about the purposes of their processing (Article 15(1)(a) of the GDPR). The related recital 63 states, among other things, that a “data subject should have the right of access to personal data that have been collected concerning him or her, and to exercise that right easily and at reasonable intervals, in order to be aware of, and verify, the lawfulness of the processing”.

3. *Restrictions to the right of access*

138. By Article 23(1) of the GDPR, EU member State legislation may restrict the scope of the obligations and rights under Articles 12 to 22 by way of a legislative measure “when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguard”, among other things, (a) national security, (b) public security, and (c) the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal

penalties – including the safeguarding against and the prevention of threats to public security. The related recital 73(1) states that “[r]estrictions concerning specific principles and the rights of information, access to and rectification or erasure of personal data ... may be imposed by Union or [m]ember State law, as far as necessary and proportionate in a democratic society to safeguard public security, ..., the prevention, investigation and prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security ... [or] other important objectives of general public interest of the Union or of a [m]ember State”, but recital 73(2) goes on to provide that those restrictions “should be in accordance with the requirements set out in the Charter and in [the Convention]”.

139. If relevant, any such legislation must, among other things, define the scope of the restrictions, and provide for the right of data subjects to be informed of any restrictions imposed – unless that could be prejudicial to its purpose (Article 23(2)(c) and (h) of the GDPR).

4. Supervisory authority

140. By Article 51(1) of the GDPR, each EU member State must provide for one or more independent public authorities to be responsible for monitoring the application of the GDPR, in order to, among other things, protect the fundamental rights and freedoms of natural persons in relation to processing. Those authorities must act with complete independence in performing their tasks and exercising their powers under the GDPR (Article 52(1)).

141. The tasks of the supervisory authority must include handling complaints lodged by a data subject, and investigating (to the extent appropriate) their subject matter and informing the complainant of the progress and the outcome of the investigation within a reasonable period; in particular, the supervisory authority must inform the complainant whether further investigation or coordination with another supervisory authority is necessary (Article 57(1)(f) of the GDPR).

142. Supervisory authorities must have “investigative powers”, including to (a) order the controller or processor to provide any information they require for the performance of their tasks, and (b) obtain from the controller or processor access to all personal data and to all information necessary for the performance of their tasks (Article 58(1)(a) and (e) of the GDPR).

143. They must also have “corrective powers”, such as the power to (a) order the controller or processor to comply with the data subject’s requests to exercise his or her rights under the GDPR, and (b) order the controller or processor to bring processing operations into compliance with the GDPR, where appropriate, in a specified manner and within a specified period, (c) impose a temporary or definitive limitation (including a ban on

processing), and (d) order the rectification or erasure of personal data or the restriction of its processing (Article 58(2)(c), (d), (f) and (g) of the GDPR).

144. Supervising authorities must also have the power to (a) bring infringements of the GDPR to the attention of the judicial authorities and (b) commence or otherwise engage in legal proceedings to enforce the GDPR (Article 58(5) of the GDPR).

5. Remedies

145. Each data subject is entitled to lodge a complaint with a supervisory authority if he or she considers that the processing of personal data relating to him or her infringes the GDPR (Article 77(1) of the GDPR).

146. Each data subject is also entitled, under the same circumstances, to an effective judicial remedy (Article 79(1) of the GDPR).

147. Each natural or legal person is also entitled to an effective judicial remedy in respect of a legally binding decision of a supervisory authority concerning them (Article 78(1) of the GDPR). Each data subject is also entitled to an effective judicial remedy if the supervisory authority does not handle a complaint or inform the data subject within three months on the progress or outcome of a complaint lodged with it under Article 77 (Article 78(2) of the GDPR).

148. Any person who has suffered material or non-material damage as a result of an infringement of the GDPR is entitled to compensation from the controller or processor (Article 82(1) of the GDPR). Article 82(2)-(4) sets out the procedure under which such compensation may be sought.

E. Law Enforcement Directive

149. Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA (OJ 2016 L 119, p. 89) (“Law Enforcement Directive” – “the LED”) governs the processing of the personal data of “natural persons” by the competent authorities for the purposes of “the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security” (Articles 1(1) and 2(1)).

150. The LED had to be transposed by May 2018 (Article 63(1)). Bulgaria did so, by way of an amendment to the 2002 Act, in March 2019 (see paragraph 85 above).

1. *Scope of application ratione materiae*

151. Article 2(3)(a) of the LED – which reflects Article 2(2)(a) of the GDPR (see paragraph 134 above) – states that the LED “does not apply to the processing of personal data ... in the course of an activity that falls outside the scope of [EU] law”. The related recital 14 states that the “[s]ince [the LED] should not apply to the processing of personal data in the course of an activity that falls outside the scope of [EU] law, activities concerning national security, activities of agencies or units dealing with national security issues and the processing of personal data by EU member States when carrying out activities that fall within the scope of Chapter 2 of Title V of the Treaty on European Union [which concern the EU’s common foreign and security policy] ... should not be considered to be activities falling within the scope of [the LED]”.

152. The CJEU has held that, under its Article 2(3)(a) read in the light of its recital 14, the LED does not apply to the processing of personal data for the purpose of protecting national security (see judgment of the CJEU of 30 January 2024 in *Direktor na Glavna direktsia ‘Natsionalna politisia’ pri MVR – Sofia*, C-118/22, EU:C:2024:97, paragraph 38).

2. *Right to access personal data*

153. By Article 14(1)(a) of the LED, EU member States must, subject to Article 15 of the LED (see paragraphs 156-159 below), provide for the right of the data subject to obtain from the controller confirmation as to whether personal data concerning him or her are being processed, and, if that is so, access to those data and information about the purposes of – and legal basis for – their processing. The related recital 43 states, among other things, that a natural person should have the right of access to data that have been collected concerning him or her, and to exercise this right easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing, and that for that right to be complied with, it is sufficient that the data subject be in possession of a full summary of those data in an intelligible form allows that data subject to become aware of those data and to verify that they are accurate and processed in accordance with the LED, so that it is possible for him or her to exercise the rights conferred on him or her by the LED.

154. In its first report on the application of the LED, published in July 2022 (COM(2022) 364 final), the European Commission recorded, on page 17, that practice had shown that the rights of access and erasure were the ones most often exercised among the rights under the LED.

155. In a November 2017 a paper entitled “Opinion on some key issues of [the LED]” (WP 258), the Working Party on the Protection of Individuals

with regard to the Processing of Personal Data (“Article 29 Working Party”)⁵ expressed the view, on page 19, that Article 14 of the LED comprises a “right of negative confirmation” (that is, a person’s right to obtain from the relevant authority confirmation that it is not processing that person’s data if that is in fact so), and that a “neither confirm nor deny” policy is only possible in the case of derogations under Article 15 of the LED.

3. Restrictions on the right of access

156. Article 15(1)(c) and (d) of the LED permits EU member States to adopt legislation restricting, wholly or in part, a data subject’s right of access “to the extent that, and for as long as such a partial or complete restriction constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests of the natural person concerned”, to protect public security or national security. In its first report on the application of the LED (see paragraph 154 above), the European Commission recorded, on page 15, that all EU member States had availed themselves of the possibility to restrict a data subject’s right of access.

157. By Article 15(2) of the LED, EU member States may adopt legislation to determine “categories of processing” that may wholly or in part fall under Article 15(1)(a) to (e).

158. In such situations, EU member States must provide for the controller to inform the data subject, without undue delay, in writing of any refusal or restriction of access and of the reasons for the refusal or the restriction, but such information may be omitted if its provision would undermine a purpose under Article 15(1). EU member States must also provide for the controller to inform the data subject of the possibility of complaining to a supervisory authority or seeking a judicial remedy (Article 15(3) of the LED).

159. By Article 15(4) of the LED, EU member States must provide for the controller to document the factual or legal reasons on which the decision to restrict is based, and that those reasons must be made available to the supervisory authorities.

160. According to the related recital 44, EU member States should be able to adopt legislation restricting (wholly or in part) data subjects’ access to their personal data to the extent that – and as long as – such a measure constitutes a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and the legitimate interests of the natural person concerned, to, among other things, protect public security or national security, but the controller should assess, by way of a concrete and individual examination of each case, whether the right of access should be partially or completely restricted. Recital 45 goes on to state that any refusal or restriction

⁵ That working party had been set up under Article 29 of the 1995 Data Protection Directive (repealed with effect from 25 May 2018 – see footnote 4 above), and was replaced by the European Data Protection Board established by Article 68 § 1 of the GDPR.

of access should in principle be set out in writing to the data subject and include the factual or legal reasons on which the decision is based, and recital 46 states that any restriction of the rights of the data subject must comply with the Charter and with the Convention, as interpreted in the case-law of the CJEU and this Court respectively, and in particular respect the essence of those rights and freedoms.

161. In the November 2017 opinion cited in paragraph 155 above, the Article 29 Working Party expressed the view, on page 20, that a “neither confirm nor deny” response could be consistent with Article 15 of the LED, but that an exemption was to be applied only where considered strictly necessary and proportionate, on a case-by-case basis, and that blanket exemptions were not to be used.

4. Indirect exercise of the right of access

162. By Article 17(1) of the LED, in the kind of situations referred to in Article 15(3) (see paragraph 158 above), EU member States must adopt measures providing that the rights of a data subject may also be exercised through the competent supervisory authority; by Article 17(2), they must provide for the controller to inform the data subject of that possibility.

163. If that right is exercised, the supervisory authority must inform the data subject “at least that all necessary verifications or a review by the supervisory authority have taken place”, and also that he or she has a right to seek a judicial remedy (Article 17(3) of the LED).

164. According to the related recital 48, in the event that the controller denies a data subject his or her right of access, the data subject should have the right to request that the national supervisory authority verify the lawfulness of the processing, and where the supervisory authority acts on behalf of the data subject, the data subject should be informed by the supervisory authority at least that all necessary verifications or reviews by the supervisory authority have taken place, and that he or she has the right to seek a judicial remedy.

165. In the November 2017 opinion cited in paragraph 155 above, the Article 29 Working Party emphasised, on pages 23-24, that this additional avenue for data subjects to exercise their rights complemented their right to complain to a supervisory authority or to seek judicial review, and that the possibility for data subjects to exercise their rights through the relevant supervisory authority was distinct from the right to complain to the supervisory authority, which had to be always available to data subjects.

166. For its part, the CJEU recently noted that the possibility under Article 17 of the LED for indirect exercise of the right of access was necessary to protect that right in situations in which its direct exercise was difficult or impossible, and that this was a mechanism by which to monitor compliance with data subjects’ rights (see judgment of the CJEU of 16 November 2023 in *Ligue des Droits Humains (Verification by the*

supervisory authority of data processing), C-333/22, EU:C:2023:874, paragraphs 44 and 48).

167. In the same judgment, the CJEU went on to say that the information disclosed to the data subject following such indirect exercise of the right of access could go beyond the minimum provided by Article 17(3) of the LED, if that was required by the need to protect the right to an effective judicial remedy (see paragraph 129 above) and was not precluded by a relevant public-interest purpose. When implementing Article 17(3) of the LED, EU member States had to allow their supervisory authorities the discretion to decide whether they could not inform the data subject (even if only in brief) of the results of their verifications (that is, the investigation carried out by the data protection authority to check whether there has been a breach of the data protection rule) and of any corrective measures taken (*ibid.*, paragraphs 65-66). If national law nevertheless required that the information given to the data subject be limited to the minimum prescribed in Article 17(3), then EU member States had to have (a) mechanisms enabling their courts to balance the need to preserve confidentiality with the data subject's procedural rights, and (b) rules enabling those courts to examine the evidence on the basis of which the supervising authorities has assessed the lawfulness of the data processing in issue. That meant, in particular, that the courts had to have before them the factual and legal reasons underlying the data controller's decision to limit the right of access – which, by Article 15(4) of the LED (see paragraph 159 above), had in any case to be documented internally (*ibid.*, paragraphs 67-70).

168. In its first report on the application of the LED (see paragraph 154 above), the European Commission recorded, on page 17, that approximately half of the supervisory authorities of EU member States had reported that they had received indirect-access requests under Article 17. Although most of those had been inadmissible, in several cases data controllers had been ordered to rectify or erase personal data or restrict their processing.

5. Supervisory authority

169. By Article 41(1) of the LED, each EU member State must provide for one or more independent public authorities to be responsible for monitoring the application of the LED, to, among other things, protect the fundamental rights and freedoms of natural persons in relation to data processing. By Article 41(3) of the LED, the authority monitoring the application of the LED can be the same as the that which monitors the application of the GDPR (see paragraph 140 above). That authority must act with complete independence in performing its tasks and exercising its powers under the LED (Article 42(1)).

170. The tasks of that supervisory authority must include (a) dealing with complaints lodged by a data subject, and investigating, to the extent appropriate, their subject matter and informing the complainant of the

progress and the outcome of the investigation within a reasonable period – in particular, in the event that further investigation or coordination with another supervisory authority is necessary, and (b) checking the lawfulness of processing (pursuant to Article 17 – see paragraph 162 above) and informing the data subject within a reasonable period of the outcome of the check (pursuant to Article 17(3) – see paragraph 163 above), or of the reasons why such a check has not been carried out (Article 46(1)(f) and (g) of the LED).

171. Supervisory authorities must have effective “investigative powers” – including at least the power to obtain from the controller or processor access to all personal data that is being processed and to all information necessary for the performance of their tasks (Article 47(1) of the LED). In its first report on the application of the LED (see paragraph 154 above), the European Commission recorded, on page 22, that nineteen supervisory authorities of EU member States had used those “investigative powers” – either on their own initiative or on the basis of a complaint.

172. Supervisory authorities must also have effective “corrective powers”, such as the power to (a) order a controller or processor to bring processing operations into compliance with the provisions adopted pursuant to the LED, where appropriate, in a specified manner and within a specified period – in particular, by ordering the rectification or erasure of personal data or the restriction of their processing, and (b) impose a temporary or definitive limitation (including a ban) on processing (Article 47(2)(b) and (c)). In its first report on the application of the LED (see paragraph 154 above), the European Commission recorded, on page 22, that the same authorities that had used their “investigative powers” (see paragraph 171 *in fine* above), had also used their “corrective powers”. The most frequently used power had been that of ordering that processing be brought into compliance with the law – including issuing orders that personal data be rectified or deleted, or that their processing be restricted.

173. Supervisory authorities must, in addition, have the power to (a) bring infringements of legal provisions adopted pursuant to the LED to the attention of judicial authorities, and (b) bring or otherwise engage in legal proceedings to enforce provisions adopted pursuant to the LED (Article 47(5)).

6. Remedies

174. By Article 52(1) and (2) of the LED, EU member States must provide for every data subject to have the right to complain to a supervisory authority.

175. In its first report on the application of the LED (see paragraph 154 above), the European Commission noted, on pages 17-18, that some of the most frequent complaints received by the data protection supervisory authorities of EU member States concerned restrictions on the right of access.

176. By Article 53(1) of the LED, EU member States must provide for the right of a natural or legal person to an effective judicial remedy in respect of

a legally binding decision issued by a supervisory authority which concerns them.

177. By Article 53(2) of the LED, each data subject also has the right to an effective judicial remedy if the competent supervisory authority does not handle a complaint or does not inform him or her within three months of the progress or outcome of a complaint lodged pursuant to Article 52.

178. By Article 54 of the LED, EU member States must provide for the right of data subjects to an effective judicial remedy where they consider that their rights laid down in provisions adopted pursuant to the LED have been infringed as a result of the processing of their personal data in breach of those provisions.

III. COUNCIL OF EUROPE INSTRUMENTS

A. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data

179. Bulgaria signed the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS 108; 1496 UNTS 65) in 1998 and ratified it in 2002, and that Convention came into force with respect to Bulgaria in January 2003. The translation of that Convention into Bulgarian was published in the Bulgarian State Gazette in March 2003 (*ДВ, бр. 26 от 21.03.2003 г., стр. 58-63*). Accordingly, it forms part of Bulgaria's domestic law and takes precedence over any conflicting provisions of domestic legislation (Article 5 § 4 of the 1991 Constitution of Bulgaria).

180. By Article 8 (a) of the 1981 Convention, any person must be enabled to “establish the existence of an automated personal data file [and] its main purposes”. By Article 8 (b), any person must be enabled to “obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file”, and, by Article 8 (d), to “have a remedy if [such] a request for confirmation ... is not complied with”.

181. By Article 9 § 2 (a) of the 1981 Convention, derogation from the provisions of Article 8 is permitted when it is “provided for by the law of the Party and constitutes a necessary measure in a democratic society in the interests of ... protecting State security, public safety, the monetary interests of the State or the suppression of criminal offences”.

182. By Article 10 of the 1981 Convention, each Party must establish appropriate remedies for violations of provisions of domestic law giving effect to the basic principles for data protection.

183. The Explanatory Report to the 1981 Convention stated, in paragraph 55, that the text of Article 9 § 2 had been “modelled after that of the second paragraphs of Articles 6, 8, 10 and 11 of the European Human

Rights Convention”, and, in paragraph 56 *in fine*, that the phrase “State security” was to be understood “in the traditional sense of protecting national sovereignty against internal or external threats, including the protection of the international relations of the State”.

B. Additional Protocol to the 1981 Convention

184. Bulgaria signed the 2001 Additional Protocol to the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS 181; 2297 UNTS 195) in 2010 and ratified it the same year; and the Protocol came into force with respect to Bulgaria in November 2010. Its translation into Bulgarian was published in the Bulgarian State Gazette also in November 2010 (*ДВ, бр. 93 от 26.11.2010 г., стр. 22-23*). It is, accordingly – like the 1981 Convention – part of Bulgaria’s domestic law and takes precedence over any conflicting provisions of domestic legislation (Article 5 § 4 of the 1991 Constitution of Bulgaria).

185. Article 1 of that Additional Protocol, entitled “Supervisory authorities”, reads, so far as relevant:

“1. Each Party shall provide for one or more authorities to be responsible for ensuring compliance with the measures in its domestic law giving effect to the principles stated in Chapters II and III of the Convention and in this Protocol.

2. a. To this end, the said authorities shall have, in particular, powers of investigation and intervention, as well as the power to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of provisions of domestic law giving effect to the principles mentioned in paragraph 1 of Article 1 of this Protocol.

b. Each supervisory authority shall hear claims lodged by any person concerning the protection of his/her rights and fundamental freedoms with regard to the processing of personal data within its competence.

3. The supervisory authorities shall exercise their functions in complete independence.

4. Decisions of the supervisory authorities, which give rise to complaints, may be appealed against through the courts.

...”

186. The Explanatory Report to the Protocol clarified, in paragraph 12, that the supervisory authority’s “powers of investigation” under Article 1 § 2 (b) comprised the possibility to ask the controller for information about the processing of personal data and to obtain it, and that such information had to be accessible, in particular, when the supervisory authority was approached by persons wishing to exercise the rights prescribed by domestic law by virtue of Article 8 of the 1981 Convention (see paragraph 180 above).

187. Paragraph 13 of the Explanatory Report specified that the supervisory authority’s “power of intervention” under Article 1 § 2 (b) could

comprise the power to oblige the controller to rectify, delete or destroy inaccurate or unlawfully collected data on its own account or if the data subject was unable to exercise those rights himself or herself.

188. Paragraph 14 of the Explanatory Report clarified that the supervisory authority also served as an intermediary between the data subject and the controller, and that everyone had to have the right to lodge a claim with the that authority in respect of his or her rights relating to the processing of personal data; that right helped to guarantee the right to an appropriate remedy under Article 8 (d) and Article 10 of the 1981 Convention (see paragraphs 180 and 182 above). A data subject could avail himself or herself of such a claim in addition to seeking a judicial remedy.

189. In a declaration deposited alongside the ratification instrument, Bulgaria stated that its national supervisory authority under Article 1 § 1 of the additional Protocol (see paragraph 185 above) was the Commission for the Protection of Personal Data (see paragraph 97 above).

C. Modernised Convention for the Protection of Individuals with regard to the Processing of Personal Data

190. The Protocol amending the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (CETS 223), whose aim is to modernise that Convention, was opened for signature in October 2018. It is not yet in force. Bulgaria signed the Protocol immediately and ratified it in December 2019 – and declared, on both occasions, that it would apply its provisions on a provisional basis (see paragraph 203 below).

191. The explanatory notes to the ratification bill (no. 902-02-24), introduced by the government and enacted by the Bulgarian Parliament in September 2019, stated that the implementation of the amending Protocol required no additional legislative measures.

1. Duty to give effect

192. By Article 4 § 1 of the modernised Convention (added by Article 6 of the amending Protocol), each Party must take measures in its law to give effect to the provisions of the amended Convention and secure their effective application; by Article 4 § 2, those measures must be taken by each Party and come into force by the time it ratifies the modernised Convention.

2. Right of access and exceptions to that right

193. By Article 9 § 1 (b) of the modernised Convention (added by Article 11 of the amending Protocol), everyone has a right to, among other things, obtain on request, at reasonable intervals and without excessive delay

or expense, confirmation of the processing of personal data relating to him or her.

194. The Explanatory Report to the amending Protocol clarified, in paragraph 74, that although the modernised Convention did not state from whom a data subject could obtain such confirmation, in most cases it would be the controller or the processor, but that in exceptional cases the exercise the right to access could involve the intermediary of the supervisory authority.

195. By Article 11 § 1 (a) of the modernised Convention (added by Article 14 of the amending Protocol) it is possible to put in place an exception to Article 9 if that exception is “provided for by law, respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society for ... the protection of national security ...”.

3. Obligation to demonstrate compliance

196. By Article 10 § 1 of the modernised Convention (added by Article 12 of the amending Protocol), each Party must provide that controllers and, where applicable, processors, take all appropriate measures to comply with the amended Convention and be able to demonstrate – subject to any legislation under Article 11 § 3 (see paragraph 200 below) – to the supervisory authority stipulated by Article 15 that data processing under their control complies with the provisions of that Convention.

4. Powers of the supervisory authorities

197. By Article 15 § 1 of the modernised Convention (added by Article 19 of the amending Protocol), each Party must provide for one or more authorities to be responsible for ensuring compliance with the provisions of that Convention.

198. By paragraph 2 (a), (c) and (d) of that Article, those supervisory authorities must have powers (a) of investigation and intervention, (b) to issue decisions with respect to violations of that Convention, and (c) to engage in legal proceedings or bring to the attention of the competent judicial authorities violations of that Convention.

199. By paragraph 4 of that Article, each competent supervisory authority must deal with requests and complaints lodged by data subjects concerning their data protection rights and keep them apprised of progress.

200. By Article 11 § 3 of the modernised Convention (added by Article 14 of the amending Protocol), when it comes to data processing for national security purposes, each Party to that Convention may provide, “by law and only to the extent that it constitutes a necessary and proportionate measure in a democratic society to fulfil such aim”, exceptions to Article 15 § 2 (a), (c) and (d).

201. The Explanatory Report to the amending Protocol clarified, in paragraph 86, that if a Party chooses to so limit the powers of a supervisory authority in relation to data processing for national security purposes, the controller is under no duty to demonstrate to that authority compliance with data protection requirements in respect of activities falling within the scope of the exception. Paragraphs 98 and 118 went on to specify that those exceptions were without prejudice to any requirements relating to the independence and effectiveness of the review and supervision mechanisms, and paragraph 117 stated that if Article 11 § 3 was triggered, the Party concerned could provide other appropriate mechanisms in respect of the independent and effective review and supervision of data processing for national security purposes.

5. Remedies

202. By Article 12 of the modernised Convention (added by Article 15 of the amending Protocol), each Party undertakes to put in place appropriate judicial and non-judicial remedies for violations of that Convention.

6. Application of the amending Protocol on a provisional basis

203. By Article 37 § 3 of the amending Protocol, a Party to the 1981 Convention may, at the time when it signs the amending Protocol or later declare that it will apply it on a provisional basis; such a declaration takes effect on the first day of the third month following the date of its receipt by the Council of Europe's Secretary General. When signing the amending Protocol (see paragraph 190 above), Bulgaria declared that it would apply it on a provisional basis (in accordance with Article 37 § 3), and confirmed that declaration in the subsequent instrument of ratification, which had been approved by its Parliament (see paragraph 191 above).

IV. OTHER RELEVANT INTERNATIONAL MATERIAL

A. Relevant Reports

1. Report by the Venice Commission

204. In its Report on the Democratic Oversight of the Security Services, adopted in 2007 and updated in 2015 (CDL-AD(2015)010), the European Commission for Democracy through Law ("the Venice Commission") noted, in particular (footnotes and internal cross-references omitted):

"251. Clearly it is necessary for individuals who claim to have been adversely affected by the exceptional powers of security and intelligence agencies, such as surveillance or security clearance, to have some avenue for redress. Quite apart from strengthening accountability, complaints may also help to lead to improved performance by the agencies through highlighting administrative failings. The requirements of human rights treaties, and especially [the Convention], with its

protections of fair trial, respect for private life and the requirement of an effective remedy must obviously also be borne in mind.

252. Plainly, though, legitimate targets of a security or intelligence agency should not be able to use a complaints system to find out about the agency's work. A complaints system should balance, on the one hand, independence, robustness and fairness, and, on the other hand, sensitivity to security needs. Designing such a system is difficult but not impossible.

253. Individuals who allege wrongdoing by the State in other fields routinely have a right of action for damages before the courts. The effectiveness of this right depends, however, on the knowledge of the individual of the alleged wrongful act, and proof to the satisfaction of the courts. As already mentioned, for a variety of reasons, the capacity of the ordinary courts to serve as an adequate remedy in security fields is limited. The case law of the European Court of Human Rights ([...]) makes it very clear that a remedy must not simply be on paper.

254. An alternative is to allow an investigation and report into a complaint against an agency by an independent official, such as an ombudsman. This is the case in e.g. the Netherlands. In other countries (for example, New Zealand and South Africa) complaints against the services are handled by an independent Inspector-General of security and intelligence as part of the office's overall oversight brief. Additionally, specific offices established under freedom of information or data protection legislation may have a role in investigating complaints against the agencies. For example, in Austria the individual usually has the possibility of complaint to the Datenschutzkommission, but if for secrecy reasons the individual has not been informed of the data (mis)use, the complaint may be raised by the Rechtsschutzbeauftragter on his/her own motion.

255. In these ombudsman-type systems, the emphasis is on an independent official investigating on behalf of the complainant. These independent offices usually exist to deal with an administrative failure by public bodies, rather than a legal error. Their investigations may give less emphasis to the complainant's own participation in the process and to transparency than would be the case with legal proceedings. Typically an investigation of this type will conclude not with a judgment and formal remedies, but with a report, and (if the complaint is upheld) a recommendation for putting matters right and future action.

256. A less common variation is for a State to use a parliamentary or expert oversight body to deal with complaints and grievances of individuals, as happens in Germany, Norway and Romania. There may be a benefit for a parliamentary oversight body in handling complaints brought against security and intelligence agencies since this will give an insight into potential failures – of policy, legality and efficiency. On the other hand, if the oversight body is too closely identified with the agencies it oversees or operates within the ring of secrecy, the complainant may feel that the complaints process is insufficiently independent. In cases where a single body handles complaints and oversight it is best if there are quite distinct legal procedures for these different roles.

257. On the whole it is preferable that the two functions be given to different bodies but that processes are in place so that the oversight body is made aware of the broader implications of individual complaints. This approach is also supported by [the Convention]. The requirement in [the Convention] Article 13 of a mechanism for remedies for alleging violations of Convention rights which is independent from the authorization process means that a State's control system, e.g. for data-processing, may pass the test of 'accordance with the law' and 'necessity in a democratic society' but

that the absence of a remedy means that there is nonetheless a violation of the Convention. As already mentioned, the ECtHR has stated that a remedy must be effective in law and fact. It should be noted in particular that the ECtHR has ruled that a data inspection authority which is independent, and which has formal competence in law to award a remedy for the holding of inaccurate, inappropriate etc. security data, but which in fact lacks the expertise to evaluate this data, is not an effective remedy within the meaning of Article 13.

258. The experience of the ECtHR in the case of *Leander v. Sweden* should also be noted. The Swedish government had argued at the time that a number of control and remedies bodies existed to prevent errors being made in security screening and to remedy any errors that were made. However, later official inquiries showed that none of the controls and remedies worked properly in this area. The people involved in each of the control/remedies systems assumed that each of the other systems was working properly. None of the controls/remedies went to the heart of the issue: the reliability and proportionality of the security assessment made of an individual. The existence of several ‘half’ control/remedies provided only a semblance of control, not its reality.

259. In some countries, not only individuals but also members of the services are permitted to bring service-related issues to the attention of an ombudsman or parliamentary oversight body. For example, in Germany officials may raise issues with the Parliamentary Control Panel and in South Africa members of the service may complain to the Inspector General.

260. Another method of handling complaints is through a specialist tribunal. This may be established to deal with complaints either against a particular agency or in relation to the use of specific powers, as in the United Kingdom (the Intelligence Services Commissioner and the Commissioner for the Interception of Communications). Or complaints may be handled in a tribunal-type procedure but by a specialist oversight body, as with the SIRC in Canada. Where the oversight body is involved in the approval process of security operations it cannot also serve as an independent complaints mechanism (see [...]). Otherwise, a tribunal of this kind has some advantages over a regular court in dealing with security- and intelligence-related complaints: it can develop a distinct expertise in the field of security and intelligence, devised for handling sensitive information. In view of the nature of the subject matter these are unlikely to involve a full public legal hearing. On the other hand, while some tribunals may give the complainant a hearing, he or she is likely to face severe practical difficulties in proving a case, in obtaining access to relevant evidence, or in challenging the agency’s version of events. To combat some of these problems special security-cleared advocates have been introduced in some countries. The critical points made before regarding the limitations applying to special advocates (see above [...]) and regarding the value of expert supervision procedures for surveillance (see above [...]) also apply here.”

2. Reports by the EU Agency for Fundamental Rights

205. Upon a request by the European Parliament, in November 2015 the EU Agency for Fundamental Rights (“FRA”) drew up a report entitled “Surveillance by intelligence services – Fundamental rights safeguards and remedies in the EU – Mapping Member States’ legal frameworks” (doi:10.2811/009038). That report analysed the laws of all of the then twenty-eight EU member States relating to such surveillance, focusing on the

supervisory mechanisms and the available remedies. It recorded, in particular, that at that time:

(a) The laws of all States permitted restrictions on the right to access one's own data on the basis of a threat to (i) national security or (ii) the objectives of the intelligence services, but there were differences in the conditions and level of restrictions. Eight States (the Czech Republic, Ireland, Latvia, Lithuania, Poland, Slovakia, Spain and the United Kingdom) did not provide for that right in relation to data processed by those services. In twenty States, that right was provided by law, but with restrictions on when it could be exercised or other qualifications. In most States (Austria, Belgium, Bulgaria, Croatia, Cyprus, Greece, Germany, Finland, France, Hungary, Italy, Luxembourg, Malta and Slovenia), the legal basis for such restrictions were the data protection laws (alone or in conjunction with specific laws) – chiefly on the grounds that the provision of information could threaten the objectives of the intelligence services or national security. In five States (Denmark, Estonia, the Netherlands, Romania and Sweden), specific laws exempted the activities of the intelligence services from the general data protection legislation. Ten States counterbalanced such restrictions by empowering supervisory bodies to (i) check whether any national security justification relied on was reasonable and/or (ii) exercise the right to access on an individual's behalf (pages 61-65 of the report).

(b) In seven States (Austria, Bulgaria, Croatia, Finland, Hungary, Slovenia and Sweden) the data protection supervisory authorities in principle had the same powers over intelligence services as those that they had with respect to other data controllers – but that did not necessarily mean that those authorities had the full range of powers otherwise available to them. In twelve States (the Czech Republic, Denmark, Estonia, Latvia, Luxembourg, Malta, the Netherlands, Portugal, Romania, Slovakia, Spain and the United Kingdom), they had no powers with respect to the intelligence services, and in nine States (Belgium, Cyprus, France, Germany, Greece, Ireland, Italy, Lithuania and Poland) they had limited powers (pages 46-51 of the report).

206. In October 2017, the FRA drew up a follow-up report entitled “Surveillance by intelligence services – Fundamental rights safeguards and remedies in the EU. Volume II, Field perspectives and legal update” (doi:10.2811/792946). That report updated the FRA's 2015 analysis of the laws of the EU member States, and supplemented it with field-based insights from interviews with experts. It recorded, in particular, that at that time:

(a) In eleven States (the Czech Republic, Denmark, Estonia, Latvia, Luxembourg, Malta, the Netherlands, Portugal, Romania, Slovakia and Spain) the data protection supervisory authorities had no competence with respect to the intelligence services; in ten States (Belgium, Cyprus, France, Germany, Greece, Ireland, Italy, Lithuania, Poland and the United Kingdom) their powers were limited; and in seven States (Austria, Bulgaria, Croatia, Finland, Hungary, Slovenia and Sweden) they had the same powers as those

that they had with respect to other data controllers. The authorities with limited powers acted as regulators of data processing for intelligence purposes. They could have an advisory role, and their role was limited to supervising compliance by the intelligence services with obligations relating to data processing. In particular, the authorities with limited powers did not look at the content of intercepted communications. They could, for instance, inspect whether the intelligence services had complied with relevant storage limits, but the law could limit their access to databases containing data collected through certain intelligence techniques. In States where the data protection supervisory authorities lacked competence with respect to the intelligence services, a specialised body supervising those services was responsible for ensuring that privacy and data protection safeguards were properly applied. In States where the data protection supervisory authorities and specialised supervisory bodies could both supervise the intelligence services, their interaction was sometimes organised by law and sometimes simply a matter of practice (pages 80-83 of the report).

(b) The data protection supervisory authorities in fourteen States could examine individual complaints. Of these, ten could give binding decisions: those in the seven States where they enjoyed the same powers with respect to the intelligence services as specialised supervisory bodies, and those in Cyprus, Greece and Italy. In four other States (Belgium, France, Germany and Ireland), the data protection supervisory authorities could deal with individual complaints or enable an individual's indirect exercise of the right to access, but could not give binding decisions. In four States (Cyprus, France, Germany and Greece), access was subject to enhanced requirements. In three States (Belgium, France and Italy), individuals could ask that authority to check whether their data were being processed by the intelligence services, and the authority would proceed with the check and inform the individual that it had taken place, but not whether and what data were being processed if such information could affect national security. If it spotted irregularities, the authority could request the intelligence service to redress them (pages 116-18 of the report).

207. In May 2023, the FRA drew up a partial update to its 2015 and 2017 reports, setting out developments that had taken place in the intelligence laws in the EU since that time (doi:10.2811/150305). The updated report recorded, in particular, that by 2023:

(a) Domestic laws passed following the 2016 EU data protection reform (which consisted chiefly in the adoption of the GDPR and the LED – see paragraphs 132 and 149 above) had led mostly to broader restrictions on (or even to the prevention of) supervision by the data protection supervisory authorities of data processing by the intelligence services. Those authorities' supervisory powers appeared to have been strengthened since 2017 in a few States only. The situation in relation to those authorities' remedial powers with respect to the intelligence services had evolved in seven States. In

Belgium, Bulgaria, Croatia, Greece and Lithuania, as a result of domestic data protection reforms made following the 2016 European reform, those authorities no longer had supervision of matters relating to national security, and had lost the power to investigate complaints relating to activities of the intelligence services. By contrast, the domestic implementation of the EU reform in Cyprus and Sweden had given those authorities new powers that had strengthened their ability to provide effective remedies.

(b) The position across the EU as of 2023 was as follows: in five States (Austria, Cyprus, Finland, Slovenia and Sweden), the data protection supervisory authorities had the same powers with respect to the intelligence services as those that they had with respect to other data controllers; in seven States (Bulgaria, France, Germany, Hungary, Ireland, Italy and Luxembourg), they had limited powers; and in fifteen States (Belgium, Croatia, the Czech Republic, Denmark, Estonia, Greece, Latvia, Lithuania, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia and Spain) they had no powers with respect to the intelligence services.

(c) The supervision framework in Bulgaria in 2023 followed the model in which the data protection supervisory authority (the Commission for the Protection of Personal Data – see paragraphs 97-102 above) had limited powers relative to those of the specialised supervisory body (the National Bureau – see paragraphs 82 (d) above). That specialised supervisory body had a leading role in that respect, with a contributory role exercised by the specialised parliamentary committee (see paragraphs 78-79 above).

B. Relevant Decision of the Committee of Ministers of the Council of Europe

208. The Committee of Ministers of the Council of Europe has so far examined the execution of the Court’s judgment in *Ekimdzhiev and Others* (cited above) in December 2022 and September 2023. It is supervising that execution under its enhanced procedure, and the proceedings before it are still pending. In its decision adopted on 21 September 2023, the Committee, among other things, “urged the authorities to develop without delay legislative amendments to strengthen the guarantees for the qualifications and independence of the members of the [National Bureau] from the authorities that the Bureau supervises before the upcoming election of a new Bureau, and, if such legislation cannot be developed before the election, to appoint sufficient members who have legal training and to avoid as far as possible the appointment of members who are law-enforcement or security services agents and may, after serving in the Bureau, regain their previous posts under a ‘revolving door’ arrangement” (see CM/Del/Dec(2023)1475/H46-10, point 4).

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

209. The applicants alleged that it was highly likely that data about them had been processed by the Agency. They complained that the impossibility of checking whether this had been so and the basis for any such processing led to uncertainty – which was in their view enhanced by the absence of clear rules on the circumstances in which the Agency could process such data and the absence of effective safeguards in that regard. The applicants relied on Article 8 of the Convention, which reads, so far as relevant:

“1. Everyone has the right to respect for his private ... life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”

A. Admissibility

1. *Compatibility* *ratione materiae*

(a) The parties' submissions

210. The Government submitted that the information which the applicants had sought from the Agency had not been personal data within the meaning of the Court's case-law. Their request had concerned the nature and type of the intelligence-gathering methods used by the Agency rather than data which could be viewed as personal to them and therefore affecting their rights under Article 8 of the Convention. The complaint was accordingly incompatible *ratione materiae* with the provisions of the Convention.

211. The applicants replied that it had been plain to both the Agency and the courts reviewing its refusal to disclose the information which they had sought that this information – whether they had been of interest to the Agency – was personal data. Their request had not concerned the Agency's working methods or the identities of its informers.

(b) The Court's assessment

212. In the initial request that Mr Kanev addressed to the Agency in June 2021, on his own behalf and on behalf of the Committee, he sought information about use by the Agency of (a) “special means of surveillance” and of (b) intelligence-gathering methods or techniques or informers (see paragraph 6 above). In its reply in late June 2021, the Agency stated that, in so far as the request concerned “special means of surveillance”, it had to be

addressed to the National Bureau, whereas, in so far as it concerned other intelligence-gathering methods or techniques and the recruitment of informers, it touched on the existence (or otherwise) of data in the Agency's databases, access to which was governed by section 36(4) of the 2007 Act (see paragraphs 7 and 67 above). Following that indication, Mr Kanev reformulated the request by asking whether the Agency's databases contained information on whether such methods or techniques had been used with respect to him or the Committee and whether members or staff of the Committee had been recruited as informers (see paragraph 8 above). In the light of that sequence of events, and of the general context in which the request was made, the Court considers that the applicants were in substance seeking confirmation whether they had been subjected to intelligence-gathering measures capable of engaging interests protected by Article 8 of the Convention, rather than information about the technical details of the methods used.

213. If the Agency had gathered intelligence on Mr Kanev, that would in principle have been apt to yield data relating to his "private life", as that term has been construed in the Court's case-law (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116; *Amann v. Switzerland* [GC], no. 27798/95, § 44, ECHR 2000-II; *Rotaru v. Romania* [GC], no. 28341/95, § 43, ECHR 2000-V; *Van Vondel v. the Netherlands*, no. 38258/03, § 48, 25 October 2007; *Haralambie v. Romania*, no. 21737/03, §§ 78-79, 27 October 2009; *Shimovolos v. Russia*, no. 30194/09, § 65, 21 June 2011; and *Kaczmarek v. Poland*, no. 16974/14, § 89, 22 February 2024). According to that case-law, the data in question can even be public information, data collected in a public place, or data concerning exclusively someone's professional or public activities – since "private life" may include activities of a professional or business nature (see *Amann*, § 65; *Rotaru*, § 43; *Van Vondel*, § 48; and *Shimovolos*, §§ 64-65, all cited above; see also *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, § 72, ECHR 2006-VII). In particular, the data in question can be data about participation in public protests (see *Association "21 December 1989" and Others v. Romania*, nos. 33810/07 and 18817/08, § 170, 24 May 2011), or even data about someone's whereabouts or comings and goings in the public sphere (see *Uzun v. Germany*, no. 35623/05, §§ 51-52, ECHR 2010).

214. If the Agency had gathered intelligence on Mr Kanev and the Committee (including by recruiting members or staff of the Committee as informers) that could have also yielded data about Mr Kanev's and the Committee's "correspondence" within the meaning of Article 8 § 1 of the Convention (see, *mutatis mutandis*, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, § 60, 28 June 2007, and *Ekimdzhiev and Others v. Bulgaria*, no. 70078/12, § 263, 11 January 2022). As construed in the Court's case-law, that term covers all sorts of private communications, whatever their content or the form that they

might take – oral communications, letters, telephone conversations or electronic exchanges (see *Michaud v. France*, no. 12323/11, § 90, ECHR 2012; *M.N. and Others v. San Marino*, no. 28005/12, § 52, 7 July 2015; and *Klaus Müller v. Germany*, no. 24173/18, § 37, 19 November 2020). In particular, it covers calls made from or received on office telephones (see *Halford v. the United Kingdom*, 25 June 1997, § 44, *Reports of Judgments and Decisions* 1997-III; *Kopp v. Switzerland*, 25 March 1998, § 50, *Reports* 1998-II; *Amann*, cited above, § 44; *Liblik and Others v. Estonia*, nos. 173/15 and 5 others, § 110, 28 May 2019; and *Algirdas Butkevičius v. Lithuania*, no. 70489/17, § 63, 14 June 2022), as well as work emails (see *Copland v. the United Kingdom*, no. 62617/00, § 41, ECHR 2007-I). The term also extends to the communications of legal persons (see *Ships Waste Oil Collector B.V. and Others v. the Netherlands* [GC], nos. 2799/16 and 3 others, § 146, 1 April 2025).

215. It should be noted in this connection that, as borne out by the facts of many cases examined by the Court, “correspondence” can be interfered with not only at the time when it is being sent or received, but also subsequently, through accessing the medium – physical or electronic – where it has been stored (see *Niemietz v. Germany*, 16 December 1992, § 32, Series A no. 251-B; *Wieser and Bicos Beteiligungen GmbH v. Austria*, no. 74336/01, § 45, ECHR 2007-IV; *Bernh Larsen Holding AS and Others v. Norway*, no. 24117/08, § 106, 14 March 2013; *Vinci Construction and GTM Génie Civil et Services v. France*, nos. 63629/10 and 60567/10, § 63, 2 April 2015; *M.N. and Others v. San Marino*, cited above, §§ 54-55; *Sérvulo & Associados – Sociedade de Advogados, RL and Others v. Portugal*, no. 27013/10, § 76, 3 September 2015; *Saber v. Norway*, no. 459/18, § 48, 17 December 2020; *Sārgava v. Estonia*, no. 698/19, § 85, 16 November 2021; and *Naumenko and SIA Rix Shipping v. Latvia*, no. 50805/14, § 45, 23 June 2022).

216. However, Mr Kanev and the Committee did not know whether the Agency had gathered intelligence on them, including intelligence coming from any informers which the Agency might have recruited from among members or staff of the Committee. The very purpose of the request which Mr Kanev addressed to the Agency – on his own behalf and on behalf of the Committee – was to obtain information on the point (see paragraphs 6 and 8 above).

217. It is true that the request was not framed as a conventional one for access to personal data held by the Agency. Nor did it expressly ask for access to particular data entries, their rectification or erasure. Its immediate object was narrower: to obtain confirmation whether the applicants had been subjected to intelligence-gathering measures or whether the Agency held information to that effect. Even so, such a request is closely connected to the protection afforded by Article 8 of the Convention, since confirmation whether an authority entrusted with safeguarding national security has

gathered intelligence on a person may constitute a necessary preliminary step for the exercise of any further rights or remedies in relation to covert data processing affecting that person's "private life" or "correspondence".

218. It would be inconsistent with the object and purpose of Article 8 of the Convention to hold that if in response to such a request the relevant authority gives an evasive or non-committal answer, or refuses to disclose whether it has gathered intelligence on the person concerned or is processing data relating to him or her, that Article finds no application unless it is positively established that such data are in fact being processed. Doing so would also run counter to the settled position that the Convention must be interpreted in a way that renders the rights it guarantees practical and effective (see *Artico v. Italy*, 13 May 1980, § 33, Series A no. 37; *Soering v. the United Kingdom*, 7 July 1989, § 87, Series A no. 161; and *Demir and Baykara v. Turkey* [GC], no. 34503/97, § 66, ECHR 2008). It would also enable the authorities to evade scrutiny in this field simply by refusing to confirm or deny whether covert measures affecting rights protected by Article 8 have been used (see, *mutatis mutandis*, *Klass and Others v. Germany*, 6 September 1978, § 36 *in fine*, Series A no. 28; *Kennedy v. the United Kingdom*, no. 26839/05, § 124, 18 May 2010; and *Roman Zakharov v. Russia* [GC], no. 47143/06, § 169, ECHR 2015). Indeed, the former Commission and the Court have both had occasion to hold, consistently with that rationale, that a refusal to advise someone of the full extent of the information about him or her that is being held by a public authority amounts, in its own right, to interference with that person's rights under Article 8 (see *Schaller Volpi v. Switzerland*, no. 25147/94, Commission decision of 28 February 1996, Decisions and Reports (DR) 84-B, p. 106, at pp. 109-10, and *Segerstedt-Wiberg and Others*, cited above, § 99; see also, *mutatis mutandis*, *Antunes Rocha v. Portugal*, no. 64330/01, §§ 64-65, 31 May 2005).

219. It follows that the Agency's refusal to disclose whether it had gathered intelligence on Mr Kanev or the Committee engaged Article 8 of the Convention. The Government's objection that the complaint is incompatible *ratione materiae* with the provisions of the Convention must accordingly be dismissed.

2. Exhaustion of domestic remedies

(a) The parties' submissions

220. The Government submitted that the applicants had not exhausted domestic remedies. Their objection comprised three lines of argument:

(a) The applicants had not sought access to personal data relating to themselves but to information about intelligence-gathering operations with respect to them. As the Supreme Administrative Court had explained when upholding the Agency's refusal to disclose such information, that kind of information did not constitute personal data.

(b) Mr Kanev’s legal challenge against the rule prescribing that information of the kind the applicants were seeking constituted an “official secret” was still ongoing (see paragraphs 32-39 above). If it resulted in the annulment of that rule, the applicants would be able to seek that information anew.

(c) The claim for judicial review of the Agency’s second refusal to disclose the information sought by the applicants was likewise still ongoing (see paragraphs 42-44 above).

221. The applicants replied that by pursuing to conclusion the claim for judicial review of the Agency’s first refusal to disclose the information that they had sought (see paragraphs 12-27 above), they had already exhausted domestic remedies. The proceedings for judicial review of the Agency’s second refusal to disclose that information (see paragraphs 42-44 above) were immaterial for the admissibility of their application to the Court; they had brought those proceedings simply to probe once again the Agency’s stance. For its part, the legal challenge against the Agency’s rule deeming that information of the kind that the applicants were seeking constituted an “official secret” could not lead to the disclosure of that information, which the Agency had later described as a “State secret”.

(b) The Court’s assessment

(i) First branch of the non-exhaustion objection

222. With reference to the first branch of the non-exhaustion objection raised by the Government, the Court notes that the applicants followed the procedural route indicated by the Agency itself. After the Agency stated that the part of the June 2021 request concerning intelligence-gathering methods or techniques and the recruitment of informers touched on the existence of data in its databases and fell to be pursued under section 36(4) of the 2007 Act, Mr Kanev reformulated the request accordingly and then sought judicial review of the ensuing refusal under section 36(9) of that Act (see paragraphs 7-12 and 67-72 above). Even if that request was not framed as a conventional one for access to personal data, it cannot be said that the applicants failed to make proper use of the remedy which, according to the Agency itself, was applicable in the circumstances of the case.

(ii) Second branch of the non-exhaustion objection

223. The second branch of the objection does not stand up to scrutiny either. Mr Kanev asked the Supreme Administrative Court to stay the proceedings in which he was seeking judicial review of the Agency’s refusal to disclose information pending the conclusion of his separate legal challenge against the rule that information of the kind that he was seeking was an “official secret”. However, the panel of the court dealing with the former case refused to stay the proceedings, holding that the resolution of the legal

challenge against the rule could not affect the lawfulness of the Agency's refusal to disclose the information sought by Mr Kanev, since the Agency itself had not cited that rule when refusing his request (see paragraphs 22 and 27 above). It is therefore unclear how a favourable outcome of the legal challenge against the rule (see paragraph 32 above) could enable the applicants to overturn the Agency's decision in their particular case. In any event, those proceedings ended with a final dismissal of that legal challenge (see paragraph 39 above). That second branch of the objection has therefore lost its relevance, if any (see, *mutatis mutandis*, *Molla Sali v. Greece* [GC], no. 20452/14, § 90, 19 December 2018; *Zoltán Varga v. Slovakia*, nos. 58361/12 and 2 others, § 112, 20 July 2021; and *Panayotopoulos and Others v. Greece*, no. 44758/20, § 90, 21 January 2025).

(iii) *Third branch of the non-exhaustion objection*

224. Nor can the third branch of the objection be sustained. As is evident from the terms of the applicants' complaint under Article 8 of the Convention (raised in September 2022, when they lodged the present application), it concerns the Agency's refusal to disclose information in July 2021 (see this judgment's preamble and paragraphs 9 and 209 above). Mr Kanev's renewed request to the Agency – made and refused in June 2023 (see paragraphs 40-41 above), about nine months after the applicants lodged the present application – and the proceedings in which Mr Kanev sought judicial review of that refusal (see paragraphs 42-44 above), are therefore of no relevance for the question of whether domestic remedies have been exhausted in relation to that complaint. The only remedies whose exhaustion is required under Article 35 § 1 of the Convention are those which relate to the breaches alleged (see, among many other authorities, *Van Oosterwijck v. Belgium*, 6 November 1980, § 27, Series A no. 40; *De Jong, Baljet and Van den Brink v. the Netherlands*, 22 May 1984, § 39, Series A no. 77; and *Paksas v. Lithuania* [GC], no. 34932/04, § 75, ECHR 2011).

225. It is true that the ongoing retention of data amounts to a continuous situation (see *Hilton v. the United Kingdom*, no. 12015/86, Commission decision of 6 July 1988, DR 57, p. 108, at p. 114; *M.M. v. the United Kingdom*, no. 24029/07, §§ 160 and 172, 13 November 2012; and *Borislav Tonchev v. Bulgaria*, no. 40519/15, § 88, 16 April 2024). However, holding that the applicants need to engage in further attempts to obtain the information that they first sought from the Agency in June 2021, and to then challenge domestically further refusals by the Agency to disclose such information, might permanently bar them from complaining in that respect to the Court – since such renewed information requests can in theory be made an indefinite number of times (see, *mutatis mutandis*, *Guzzardi v. Italy*, 6 November 1980, § 80, Series A no. 39; *Nenov v. Bulgaria*, no. 33738/02, § 38, 16 July 2009; *Naydenov v. Bulgaria*, no. 17353/03, § 58 *in fine*, 26 November 2009; *United Macedonian Organisation Ilinden and Others v. Bulgaria* (no. 2),

no. 34960/04, § 27, 18 October 2011; and *United Macedonian Organisation Ilinden-PIRIN and Others v. Bulgaria* (no. 2), nos. 41561/07 and 20972/08, § 70, 18 October 2011). Moreover, the possibility of asking a public authority to reconsider a decision that it has already taken is normally not an effective remedy (see *Roseiro Bento v. Portugal* (dec.), no. 29288/02, ECHR 2004-XII; *United Macedonian Organisation Ilinden and Others* (no. 2), cited above, § 27 *in fine*; *United Macedonian Organisation Ilinden-PIRIN and Others* (no. 2), cited above, § 70 *in fine*; and *Vasil Vasilev v. Bulgaria*, no. 7610/15, § 112 *in fine*, 16 November 2021).

226. In any event – and perhaps most importantly in the present case – the proceedings for judicial review of the Agency’s second refusal to disclose the information in June 2023 ended in July 2024, and, in the event, their outcome provided no redress to the applicants – they led simply to a reiteration of the Agency’s two earlier refusals to disclose the information sought by them (see paragraphs 45-50 above). That third branch of the objection has therefore likewise lost its relevance, if any (see, *mutatis mutandis*, *Molla Sali*, § 90; *Zoltán Varga*, § 112; and *Panayotopoulos and Others*, § 90, all cited above).

(iv) *Conclusion*

227. It follows that the Government’s objection that domestic remedies have not been exhausted must be dismissed as well.

3. *The Court’s conclusion on the admissibility of the complaint*

228. It was already established that this complaint is not incompatible *ratione materiae* with the provisions of the Convention and that the applicants have exhausted domestic remedies with respect to it (see paragraphs 212-219 and 222-227 above). The complaint is not manifestly ill-founded or inadmissible on other grounds either. It must therefore be declared admissible.

B. Merits

1. *Existence of an interference with rights protected under Article 8 of the Convention*

(a) *The parties’ submissions*

229. The applicants contended that it remained unclear whether the Agency had gathered intelligence on them; it had neither confirmed nor denied that – either at domestic level or in its reply in connection with the proceedings before the Court. There was, nonetheless, a strong suspicion that it had in fact done so. It had been fully possible for the Agency to answer that question, even in relation to members or staff of the Committee. The possibility of obtaining information about the use of “special means of surveillance” though the National Bureau was ineffective, since the Bureau

had to in turn get that information from the Agency, and the Agency deemed such information to be classified. The 2007 Act did not lay down sufficient safeguards, which meant that anyone could have their data collected and stored by the Agency (which had broad powers and operated in secret). Since no one could check whether the Agency had indeed collected and stored his or her data, it was reasonable to surmise that the applicants had also been of interest to it.

230. The Government observed that the Agency had not confirmed that it had gathered or stored data relating to the applicants, and that there was no indication that it had in fact done so (apart from data relating to access-to-information requests by the applicants and related judicial review proceedings). The applicants' misgivings on that point were abstract and baseless, being founded just on statements made by the Minister of Internal Affairs relating to politicians and participants in the 2020-21 anti-government protests. The applicants fell in neither of those categories, and their supposition that they might have been of interest to the Agency was vague and far-fetched. The reasons that the Agency had given to refuse Mr Kanev's request and those that the courts had then given to dismiss his claim for judicial review of that refusal contained nothing that could suggest otherwise. There had, then, been no interference with the applicants' Article 8 rights. Moreover, as attested by the National Bureau's response (see paragraph 31 above), no "special means of surveillance" had been employed with respect to Mr Kanev throughout the period in question. No such means could be used with respect to the Committee, since under Bulgarian law such means could be deployed only with respect to individuals, not legal persons. There was therefore no evidence that data about the applicants had been obtained by the Agency in the course of its operations.

231. The Government further argued that the Agency's refusal to disclose the information sought by the applicants had not interfered with their Article 8 rights either, since the applicants' request had concerned no personal data of theirs.

(b) The Court's assessment

232. In the particular circumstances of the present case, the Agency's refusal to disclose whether it had gathered intelligence on Mr Kanev or the Committee amounted, in its own right, to an interference with their rights under Article 8. The applicants' request concerned the possible use of covert intelligence-gathering measures capable of affecting their "private life" and "correspondence", and the Agency's response was in substance one of refusal to confirm or deny whether such measures had been applied. Such a refusal may itself constitute an interference within the meaning of Article 8 (see *Segerstedt-Wiberg and Others*, cited above, § 99, and, *mutatis mutandis*, *Centrum för rättvisa v. Sweden* [GC], no. 35252/08, §§ 244-45, 25 May 2021,

and *Big Brother Watch and Others v. the United Kingdom* [GC], nos. 58170/13 and 2 others, §§ 330-31, 25 May 2021).

2. *Justification for the interference*

233. Under the second paragraph of Article 8 of the Convention, such interference can be justified only if it was “in accordance with the law” and “necessary in a democratic society” to attain one or more of the legitimate aims set out in that paragraph. It otherwise entails a breach of that Article.

(a) *The parties’ submissions*

234. The applicants reiterated that the 2007 Act did not lay down effective safeguards against the arbitrary use of “special means of surveillance”, which had enabled the Agency to operate in an unforeseeable manner. By refusing to disclose whether it had gathered intelligence on the applicants, the Agency had made it impossible for them to check the nature, scope and duration of any such interference with their rights. Contrary to what the Government claimed, the Agency had declined to answer that question. It was true that States had a wide margin of appreciation in that sphere, but they were still required to have in place effective guarantees against abuse. The interference could not be justified with reference to national security, since the applicants had not sought information about any techniques or methods used for surveillance, or details about that; Mr Kanev’s request had been formulated quite generally. Moreover, in Bulgaria the concept of national security had a long history of misuse. The interference had therefore not been “necessary in a democratic society”.

235. The Government submitted that any interference with the applicants’ Article 8 rights had been “in accordance with the law”, since the Agency’s refusal to disclose information about any intelligence-gathering in relation to them had been based on the provisions of the 2007 Act, which were clear and accessible. The interference had sought to safeguard national security, since any publicity could render the Agency’s methods and techniques ineffective. In view of the nature of the information sought by the applicants, the refusal to disclose it had also been proportionate and had fallen within the authorities’ margin of appreciation, which was wide in that sphere.

(b) *The Court’s assessment*

(i) *Was the interference “in accordance with the law”?*

(α) *General principles*

236. There can be no doubt about the necessity, for the purpose of protecting national security, for the Contracting States to have laws granting their competent authorities the power to collect and store in databases not accessible to the public information about persons (see *Leander*, cited above,

§ 59). However, the phrase “in accordance with the law” does not just mean that an interference with rights under Article 8 of the Convention must have a basis in domestic law, but also refers to the quality of that law – requiring it to be accessible, foreseeable and compatible with the rule of law (see *Kopp*, § 55; *Amann*, §§ 50 and 56; *Rotaru*, § 52; and *Segerstedt-Wiberg and Others*, § 76, all cited above). In the sphere under consideration, this entails, in particular, the availability of effective safeguards against arbitrariness and abuse. This is because (a) a surveillance system not open to scrutiny by the persons concerned or the public at large (because it is being operated by the authorities in secret) presents obvious risks in that respect, and because (b) a surveillance system designed to safeguard national security may undermine or even destroy democracy on the pretence of defending it (see *Leander*, § 60; *Amann*, § 56; *Rotaru*, §§ 55 and 59; *Antunes Rocha*, § 76; and *Segerstedt-Wiberg and Others*, § 76, all cited above).

237. Naturally, in this sphere, as in others, the requisite safeguards will depend on the nature and extent of the interference (see, among other authorities, *P.G. and J.H. v. the United Kingdom*, no. 44787/98, § 46, ECHR 2001-IX; *C.G. and Others v. Bulgaria*, no. 1365/07, § 45, 24 April 2008; *El Haski v. Belgium*, no. 649/08, § 107, 25 September 2012; and *Giuliano Germano v. Italy*, no. 10794/12, § 94, 22 June 2023). The context within which the interference is taking place is also a material consideration (see *I.R. and G.T. v. the United Kingdom* (dec.), nos. 14876/12 and 63339/12, § 61 *in fine*, 28 January 2014; *Saeed v. Denmark* (dec.), no. 53/12, § 35, 24 June 2014; and *Mirzoyan v. the Czech Republic*, nos. 15117/21 and 15689/21, § 81 *in fine*, 16 May 2024).

238. For interferences of the kind at issue in the present case, the impossibility for the applicants to (a) access data relating to them that is being processed by an authority entrusted with safeguarding national security, and even to (b) obtain a clear response to their enquiry about whether such processing has taken place, cannot in itself raise concerns under Article 8 of the Convention – since it is the very absence of such information that can ensure the efficacy of that authority’s work (see *Leander*, § 66; *Segerstedt-Wiberg and Others*, § 102; and *Dalea*, all cited above; see also, *mutatis mutandis*, *Antunes Rocha*, cited above, § 64). This applies even more to information that could make it possible to discover the identities of people who have collaborated with the Agency – since that might not only put their safety at risk but also discourage future collaboration with the Agency.

239. It is not the Court’s role to devise comprehensive rules in this sphere. However, since it cannot shirk its responsibility to ascertain whether the interference was “in accordance with the law”, it must elucidate the nature and scope of the obligations which this phrase implies in that sphere – thus fulfilling its task under Articles and 19 and 32 § 1 of the Convention to ensure the observance of the engagements undertaken by the Contracting States in it, and to interpret the Convention – in particular, the rights and freedoms set

out in its Section I (see *Humpert and Others v. Germany* [GC], nos. 59433/18 and 3 others, § 69, 14 December 2023).

240. In the present case, which revolved at domestic level around the application of Bulgaria's special data protection regime in the domain of intelligence-gathering for national security purposes, possibly also through covert surveillance, it is appropriate to approach the question of what sort of safeguards can ensure effective protection against arbitrariness and abuse by considering:

(a) the solutions (as they have emerged in EU data protection law, in the treaties resulting from the work of the Council of Europe in that sphere (which Bulgaria has ratified) and in the domestic laws of various Contracting States – see paragraphs 156, 158-159, 162-172, 187-188, 194 *in fine*, 201 and 205-207 above) devised in data protection law in relation to situations of the kind arising here. Indeed, when assessing data processing under Article 8 of the Convention, the Court often takes into account the principles contained in that law (see *L.B. v. Hungary* [GC], no. 36345/16, § 123, 9 March 2023, and *Ships Waste Oil Collector B.V. and Others*, cited above, § 155 *in fine*); and

(b) the solutions flowing from the Court's own case-law in respect of functionally analogous scenarios, which involve the same sort of considerations as those that arise in the present case – notably that of the bulk interception of communications.

241. In the area of bulk interception of communications, national security considerations can likewise as a matter of course preclude the possibility of notifying the persons concerned that data relating to them has been acquired and is being held. In the light of that, the Court has held that the absence of such notification can be counterbalanced by effective supervision and by a complaints mechanism which does not depend on such notification and permits anyone who suspects that his or her communications have been intercepted to bring proceedings before an authority which: (i) while not necessarily judicial, is independent of the executive; (ii) ensures fair proceedings, offering, in so far as possible, an adversarial process; and (iii) can give reasoned and legally binding decisions with regard to, *inter alia*, the destruction of unlawfully obtained or stored intercept material (see *Centrum för rättvisa*, §§ 271-73, and *Big Brother Watch and Others*, §§ 357-59, both cited above). On that basis, the Court has accepted as satisfactory:

(a) independent supervision authorities which: (i) enjoy access to all relevant material; (ii) are empowered to review the interception, analysis, use and destruction of such material by the intelligence services and to direct that any collected data be destroyed; (iii) can examine the necessity and proportionality of the interference with Convention rights that may be occasioned by the bulk interception of communications; and (iv) regularly

exercise those powers in practice (see *Centrum för rättvisa*, §§ 345-53, and *Big Brother Watch and Others*, §§ 406-12, both cited above); and

(b) *ex-post-facto*-review mechanisms which: (i) can be triggered without the persons concerned having to demonstrate that they may have been affected by a bulk interception operation; (ii) are independent, in particular *vis-à-vis* the intelligence-gathering activities that they are called upon to review; (iii) can obtain and scrutinise all relevant material; (iv) can duly consider whether the relevant operations of the intelligence services comply with the Convention; and (v) can respond to complaints by way of legally binding decisions which can, *inter alia*, direct that intercept material is to be destroyed and contain publicly available reasons, or at least reasons accessible to special security-cleared counsel (see *Centrum för rättvisa*, §§ 354-64, and *Big Brother Watch and Others*, §§ 413-14, both cited above).

242. The above-mentioned solutions, which largely overlap, suggest that whenever it is legitimate and proportionate to curtail or do away with transparency in the processing of data by a public authority because that could frustrate or even defeat the purpose of that processing or another valid interest (as is frequently the case with data processing by the security and intelligence services), the only feasible way to prevent arbitrariness or abuse in relation to that processing – and thus ensure that it is “in accordance with the law” – is to have in place an indirect-access mechanism or a supervision mechanism, or a combination of such mechanisms, capable of making up for the impossibility for the persons concerned to seek redress directly and in full knowledge of the facts. That mechanism must ensure sufficiently robust independent scrutiny of the relevant data processing; its proper functioning depends on the effective investigative, corrective and remedial powers of the independent authority carrying out that scrutiny. More specifically, that authority must: (a) be sufficiently independent; (b) ensure fair proceedings, offering, in so far as possible, an adversarial process; (c) be capable of obtaining and scrutinising all relevant material; (d) be capable of duly considering whether the relevant data processing is Convention-compliant; and (e) be capable of giving reasoned and legally binding decisions with regard to the processing of the relevant data. The mechanism must, of course, also operate effectively in practice.

243. That was also the broad logic underlying the Court’s analysis in *Leander* (cited above, §§ 61-66), *Segerstedt-Wiberg and Others* (cited above, §§ 102-03) and *Dalea* (cited above).

(β) Application of those principles

244. The Agency’s refusal to disclose whether it had gathered intelligence on Mr Kanev or the Committee – including intelligence obtained by recruiting members or staff of the Committee as informers – was based on the relevant provisions of the 2007 Act and was upheld by the Bulgarian

courts (see paragraphs 7, 9-11, 19 and 23-27 above). It can therefore be accepted that the interference was lawful in terms of Bulgarian law.

245. The question remains, then, whether the interference met the other requirements arising from the phrase “in accordance with the law”, as outlined in paragraphs 236-243 above – in particular, whether it was surrounded by effective safeguards against arbitrariness and abuse.

246. The assessment of this question necessarily entails a degree of abstraction (see *Kruslin v. France*, 24 April 1990, §§ 31-32, Series A no. 176-A, and *Huvig v. France*, 24 April 1990, §§ 30-31, Series A no. 176-B). It indeed requires an examination of the entire system put in place by the respondent State – since a shortcoming in one respect might be offset by a safeguard present elsewhere (see *I.R. and G.T. v. the United Kingdom*, § 60, and *Saeed*, § 35 *in fine*, both cited above).

247. The potential safeguards in relation to the processing by the Agency of operational data relating to the applicants are: (a) the proceedings for judicial review of its refusal to disclose whether it was processing such data; (b) possible supervision of data processing by the Agency by the Commission for the Protection of Personal Data; (c) the supervision of some parts of the Agency’s work by the National Bureau; (d) the supervision of the Agency’s work by a special parliamentary committee and by the Parliament as a whole; and (e) the supervision of the Agency’s work by the government and the President of the Republic.

– *Judicial review of the Agency’s refusal to disclose whether it was processing data relating to the applicants*

248. The proceedings for judicial review of the Agency’s refusal to disclose whether it had gathered intelligence on the applicants, or held information to that effect in its databases – which the applicants brought under section 36(9) of the 2007 Act, following the Agency’s decision pursuant their request under section 36(4) (see paragraphs 12 and 67-72 above) – cannot be viewed as an effective safeguard.

249. Firstly, the courts that dealt with those proceedings did not see the material (if there was indeed any) to which the Agency’s decision related (contrast *Brinks v. the Netherlands* (dec.), no. 9940/04, 5 April 2005, and *Das Universelle Leben Aller Kulturen Weltweit e.V. v. Germany* (dec.), no. 60369/11, § 24, 17 November 2015). On the contrary, they declined to compel the Agency to produce such material – even for their own inspection – on the basis that it was not needed in order to examine the lawfulness of the Agency’s decision (see paragraphs 14 (b), 17 and 24 above). That deficiency is all the more significant in a case such as the present one, where the very question in issue was whether the Agency had gathered intelligence on the applicants or was holding information capable of engaging their rights under Article 8.

250. It is true that under section 39a, respectively section 39(3)(3), of the Protection of Classified Information Act 2002, litigants and their lawyers have the right to access classified information relating to a case in which they are involved without undergoing security screening if that is necessary for the defence of their constitutional rights (see paragraphs 114 *in fine* and 115 above). However, the discussions in the Legal Affairs Committee of the Parliament during the formulation of the final wording of section 39a and the few reported cases relating to the application of sections 39(3)(3) and 39a by the administrative courts suggest that those provisions can only be relied on when the classified information has already been produced by the Agency (see paragraphs 117-121 above). As noted in the previous paragraph, that was not the situation here. Nor is there any indication that arguments based on sections 39(3)(3) and 39a would have enabled the applicants, by indirect procedural means, to secure disclosure of material which the Agency had refused even to confirm existed. It should also be noted in this connection that the Supreme Administrative Court held that since the whole case revolved precisely around the question whether the information sought by the applicants was to be disclosed, it was not appropriate to obtain that result through evidential requests made in the proceedings themselves (see paragraph 24 above).

251. Secondly, the courts that dealt with those proceedings did not examine whether the disclosure of such information could in fact harm or endanger any public interest – in particular, national security. They deferred fully to the Agency’s assessment of that point – even though they remained entirely unaware of the specific reasons that had led the Agency to form the view that it could not disclose such information, and indeed of whether any individual assessment had been carried out in the applicants’ case (see paragraphs 19 and 25 above). The Supreme Administrative Court adhered to the same position in the proceedings for judicial review of the Agency’s second refusal in June 2023, holding that the Agency was under no duty to give any reasons on points of fact (see paragraphs 43 and 47 above). It thus appears that the domestic courts did not undertake any scrutiny capable of testing whether the Agency’s refusal to confirm or deny intelligence-gathering with respect to the applicants was justified in the particular circumstances of the case.

252. Thirdly, in so far as the second applicant is concerned, the effectiveness of that avenue was further reduced by the fact that section 36 of the 2007 Act concerns personal data, whereas the Committee is a legal person. Although the Committee could rely on Article 8 in respect of its “correspondence”, it does not appear that proceedings under section 36 were capable of affording it equivalent redress in relation to a refusal to disclose whether it had been subjected to intelligence-gathering measures or whether information to that effect was being held by the Agency (compare *Ekimdzhiev and Others*, cited above, § 354).

– *Supervision by the Commission for the Protection of Personal Data*

253. Nor does it appear that an effective safeguard could be afforded by Bulgaria's main data protection supervisory authority – the Commission for the Protection of Personal Data.

254. Supervisory bodies of that sort can furnish an effective safeguard with respect to data processing by the authorities for law-enforcement and intelligence purposes (see *Breyer v. Germany*, no. 50001/12, §§ 105 and 107, 30 January 2020, and *Ringler v. Austria* (dec.) [Committee], no. 2309/10, §§ 72-79, 15 May 2020). But they can only do so if they can directly access those data and any related information, so as to be able to check whether they are being processed in a manner that is consistent with the relevant data protection principles. In a recent case against Hungary, an investigation by such a supervisory body in which it could not access directly data processed by the national security services was not considered to be an effective safeguard because the absence of direct access had prevented proper scrutiny by it (see *Hüttl v. Hungary* [Committee], no. 58032/16, §§ 15-18, 29 September 2022).

255. In Bulgaria, the role of that Commission with respect to data processing by the Agency for operational purposes does not appear to be clearly defined. It is true that section 37 of the 2007 Act, as originally enacted, empowers that Commission to supervise the processing of personal data by the Agency in the manner provided by the 2002 Act (see paragraph 77 above). At the same time, section 1(5) of the 2002 Act itself (as amended in March 2019) states that that Act does not apply to the processing of personal data for national security purposes unless that is expressly prescribed elsewhere – the stated rationale being that the elaborate data protection regime instituted by EU law, especially since the adoption of the GDPR and the LED, and reflected in the 2002 Act, does not cover the processing of personal data for activities relating to the protection of national security (see paragraph 88 above). It is therefore unclear whether section 37 of the 2007 Act can be read to mean that the 2002 Act's strictures apply to the processing of such data by the Agency for operational purposes (or that the 2002 Act applies only to data processing by the Agency for other purposes – such as staff administration and public procurement), and that that Commission can exercise the investigatory and remedial powers that it has under the 2002 Act with respect to data obtained by the Agency in the course of its operations.

256. Nor is there any indication that – apart perhaps from a 2009 audit of the Agency in connection with preparations for the future implementation of the Schengen Information System – that Commission has ever checked how the Agency processes operational data, and in particular, whether it duly follows the statutory rules and the regulations which govern that matter (see paragraphs 62-65 and 102 above; also compare *Ekimdzhiev and Others*, cited above, §§ 346 and 412; also contrast, *mutatis mutandis*, *Centrum för rättvisa*,

§ 351, and *Big Brother Watch and Others*, §§ 409-10, both cited above). On the contrary, the (apparently) only case in which that Commission was invited to look into the matter in question indicates that it was of the view that data resulting from surveillance carried out by the Agency did not amount to personal data, and that such operations by the Agency were not for it to supervise (see paragraph 90 above).

257. A further limitation flows from the fact that the Commission for the Protection of Personal Data may scrutinise only the processing of data relating to individuals – not data relating to legal persons such as the Committee (see paragraph 87 above; also compare *Ekimdzhiev and Others*, cited above, § 331).

– *Supervision by the National Bureau*

258. The first thing which should be noted about the National Bureau is that it may supervise only the use of “special means of surveillance” – not all sorts of intelligence gathering and related data processing by the Agency (see paragraph 82 (d) above). That limit on the Bureau’s role was illustrated by the facts of the present case, in which the Agency responded itself to the part of Mr Kanev’s request relating generally to intelligence-gathering methods or techniques, and referred him to the Bureau only so far as his request concerned “special means of surveillance” (see paragraphs 6-11 above). Supervision by the Bureau is therefore not a safeguard with respect to the overall manner in which the Agency processes operational data. Nor is the Bureau required to check whether “special means of surveillance” have been used with respect to legal persons such as the Committee (see *Ekimdzhiev and Others*, cited above, § 349).

259. Moreover, the Bureau’s effectiveness – even in relation to the processing of data about individuals obtained as a result of the use of “special means of surveillance” – is undermined by several shortcomings already identified in *Ekimdzhiev and Others* (cited above, §§ 339-44) that have apparently not been rectified since that judgment became final in April 2022 (see paragraph 208 above):

(a) the absence of a guarantee that all Bureau members are sufficiently independent *vis-à-vis* the authorities that they must supervise – in particular, the Agency (*ibid.*, §§ 339-41);

(b) misgivings about the qualifications of some Bureau members (*ibid.*, § 342);

(c) the Bureau’s inability to secure unfettered access to all relevant material held by, in particular, the Agency (*ibid.*, § 343); and

(d) the Bureau’s lack of any power to order remedial measures, such as the destruction of surveillance material (*ibid.*, § 344).

260. Indeed, it seems that all the Bureau did in the present case by way of investigation was to write to the Agency to enquire whether it had deployed “special means of surveillance” in relation to Mr Kanev and then review the

Agency's reply (see paragraph 31 above; also contrast *Big Brother Watch and Others*, cited above, §§ 408 and 410).

– *Supervision by a special parliamentary committee and the Parliament as a whole*

261. The special parliamentary committee tasked with supervising the Agency's work – the same committee that was in issue in *Ekimdzhiev and Others* (cited above, § 125) – is empowered to deal with individual cases, but it cannot order remedial measures; if it detects irregularities, it can only bring them to the attention of the prosecuting or other relevant authorities (see paragraph 78 above). Moreover, that committee's members are not required to have any legal qualifications or experience (see *Ekimdzhiev and Others*, cited above, § 414). Nor does it seem that it has in practice exercised detailed and regular control over the Agency's data processing operations or involved itself in the Agency's day-to-day work (compare *Ekimdzhiev and Others*, cited above, § 345, and, *mutatis mutandis*, *Szabó and Vissy v. Hungary*, no. 37138/14, § 82, 12 January 2016; also contrast *Leander*, cited above, §§ 40 and 65).

262. There is no indication that the Agency's head, deputy heads or officers have ever been called to the Bulgarian Parliament to report specifically on whether the Agency has acted lawfully when processing data obtained as a result of its operations (see paragraph 79 above). In any event, such general parliamentary supervision can hardly be viewed as sufficient to prevent individual abuses.

– *Supervision by the government and the President of the Republic*

263. There is no indication that the Agency has discussed specifically (in reports to the government or the President of the Republic) the way in which it processes data obtained as a result of its operations (see paragraphs 80-81 above). In any event, such general political oversight can hardly be considered independent (see, *mutatis mutandis*, *Association for European Integration and Human Rights and Ekimdzhiev*, § 87, and *Szabó and Vissy*, § 75, both cited above), or sufficient to prevent individual abuses.

– *Conclusion*

264. The above analysis leads to the conclusion that the applicants did not enjoy the minimum degree of protection against arbitrary and unlawful processing by the Agency of data about them. The interference with their rights under Article 8 of the Convention was therefore not in accordance with a "law" meeting the requirements of the second paragraph of that Article.

(ii) *Purpose and necessity of the interference*

265. In the light of the above conclusion, it is not necessary to rule on the question of whether the interference pursued a legitimate aim and was “necessary in a democratic society” to attain that aim (see *Kopp*, § 76; *Amann*, §§ 63 and 81; *Rotaru*, § 62; *Antunes Rocha*, § 79; and *Zoltán Varga*, § 172, all cited above).

(iii) *Final conclusion*

266. It follows that there has been a breach of Article 8 of the Convention.

II. ALLEGED PROCESSING OF DATA ABOUT THE APPLICANTS’ POLITICAL OPINIONS, AFFILIATIONS AND ACTIVITIES

267. The applicants complained that the Agency had unjustifiably collected data on their political opinions, affiliations and activities. They relied on Articles 10 and 11 of the Convention, which read, so far as relevant:

Article 10 (freedom of expression)

“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. ...

2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”

Article 11 (freedom of assembly and association)

“1. Everyone has the right to freedom of peaceful assembly and to freedom of association with others ...

2. No restrictions shall be placed on the exercise of these rights other than such as are prescribed by law and are necessary in a democratic society in the interests of national security or public safety, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others. ...”

A. The parties’ submissions

268. The Government contended that the Agency had collected no data on the political opinions, affiliations or activities of the applicants. It was, moreover, unclear how that could, in any event, have affected their exercising their rights under Articles 10 or 11 of the Convention. There had, then, been no interference with those rights. In the alternative, they argued that any such interference had been lawful and justified, since the Agency’s decision to

withhold information on the point had been based on clear and accessible rules that were meant to safeguard national security, and proportionate – in particular, in view of its minimal or even non-existent impact on the applicants.

269. The applicants conceded that they could not know for certain whether the Agency had gathered and was holding intelligence on them. They had, however, a strong suspicion that this was so, and in their view any such data would inevitably relate to their political opinions, affiliations and activities. The Agency's refusal to disclose whether this was so had therefore also amounted to interference with their rights under Articles 10 and 11 of the Convention. That interference had been unlawful and unjustified for the same reasons as the interference with their Article 8 rights.

B. The Court's assessment

270. The Court has had occasion to hold that the storage of data relating to political opinions, affiliations and activities which is unjustified under Article 8 § 2 of the Convention inevitably also constitutes an unjustified interference with the rights protected under Articles 10 and 11 of the Convention (see *Segerstedt-Wiberg and Others*, cited above, § 107). It has also held that data revealing political opinions – such as information about participation in peaceful protests – attract a heightened level of protection (see *Catt v. the United Kingdom*, no. 43514/15, §§ 112 and 123, 24 January 2019, and *Glukhin v. Russia*, no. 11519/20, § 76, 4 July 2023).

271. In this case, however, it remains unknown what data about the applicants, if any, have been collected by the Agency. It is therefore a matter of speculation whether any such data relate to their political opinions, affiliations or activities (contrast *Segerstedt-Wiberg and Others*, § 107, and *Catt*, §§ 122-23, both cited above). Since the availability of effective safeguards in relation to the processing of those data was examined comprehensively under Article 8 § 2 (see paragraphs 248-264 above), there is no need to do so also from the perspective of Articles 10 and 11. Indeed, the parties advanced no arguments in respect of that issue in addition to those that they advanced under Article 8 § 2 (see paragraphs 268-269 above).

272. The admissibility and merits of this complaint do not therefore require separate examination.

III. ALLEGED BREACH OF THE RIGHT TO RECEIVE INFORMATION

273. The applicants complained that the Agency had unjustifiably withheld the information sought by them. They again relied on Article 10 of the Convention, the relevant part of which has been set out in paragraph 267 above.

A. The parties' submissions

1. *The Government*

274. The Government submitted that that this complaint was likewise incompatible *ratione materiae* with the provisions of the Convention, since it was unclear how the information sought by the applicants – which touched on the Agency's methods and the identities of its informers – could relate to the exercise of their right to freedom of expression under Article 10 of the Convention.

275. The Government went on to argue that there had been no interference with the applicants' right to receive information. Firstly, they had not spelled out the purpose of their request to the Agency, and the information sought by them had been far from instrumental in respect of their freedom of expression – assuming their idea had been to provoke a public debate on access to data obtained through covert surveillance. Secondly, the information they had sought had concerned the Agency's methods rather than data about them. The authorities had correctly assessed that that information was to be withheld because its disclosure could harm national security. That disclosure would not have been in the public interest – irrespective of the applicants' role as public watchdogs.

276. In the alternative, the Government argued that any such interference had been lawful and undertaken in pursuit of a legitimate aim, for the same reasons as the alleged interference with the applicants' Article 8 rights (see paragraph 235 above). The interference had also been proportionate, since it had been justifiable for the kind of information being sought by the applicants to remain secret. Mr Kanev had been told by the National Bureau that no "special means of surveillance" had been used against him, and no such means could have been used with respect to the Committee.

2. *The applicants*

277. The applicants replied that the Government was mischaracterising the nature of the information that they had sought.

278. According to them, the Agency's refusal to disclose that information had interfered with their right to receive information. The disclosure of that information – which had not concerned the Agency's methods as such – would have ensured transparency on a matter of interest to society as a whole, and would have enhanced trust in the security services following revelations of abuse by an official well familiar with their work. The applicants' role as public watchdogs was also of importance. The purpose of their request to the Agency had been self-evident and sufficiently clear from the request itself. They had later explained in detail the background to the request in their submissions in the judicial review proceedings.

279. The applicants went on to argue that the Agency’s refusal to disclose the information had not been “necessary in a democratic society”. The 2007 Act did not contain effective safeguards against misuse of the Agency’s broad powers and data processing capabilities. The suspicion that “special means of surveillance” were being misused was widespread in Bulgaria and could not be allayed by the existing notification mechanism.

B. The Court’s assessment

280. The Agency’s refusal to disclose whether it had gathered intelligence on the applicants was reviewed in detail under Article 8 of the Convention (see paragraphs 212-219, 232-233 and 236-266 above). There is, then, no need to examine the admissibility or merits of their related complaint under Article 10 of the Convention, which – as can be seen from the way in which it was formulated and from the applicants’ submissions in relation to it (see paragraphs 273 and 279 above) – amounts to a restatement of the complaint under Article 8 of the Convention, and gives rise to no separate issue over and above that arising under Article 8 of the Convention (see, *mutatis mutandis*, *Silver and Others v. the United Kingdom*, 25 March 1983, § 107, Series A no. 61, and *Big Brother Watch and Others*, cited above, § 516).

IV. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

281. The applicants also complained that they had not had an effective remedy in respect of the impossibility of obtaining from the Agency information about whether it was processing data relating to them. They relied on Article 13 of the Convention, which reads:

“Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.”

A. The parties’ submissions

282. The Government pointed out that the applicants had been able to seek judicial review of the Agency’s refusal to disclose the information that they had sought. However, as had transpired during those proceedings, that information had not amounted to personal data, which had meant that they had to rectify their request to the Agency. They had failed to do so, instead simply reiterating the request two years later – apparently well aware that it would be met with the same response. It was still open to them to reformulate their request. The fact that the judicial review proceedings had not yielded the outcome sought by them did not mean that such proceedings did not constitute an effective remedy.

283. The applicants submitted that the three sets of judicial review proceedings that they had brought had not furnished them with an effective remedy in respect of the Agency's refusal to disclose the information sought by them – mainly because the courts had not required the Agency to articulate the national security risks that could result from such disclosure. The only judgment compelling the Agency to provide such justification had been the one given by the Sofia City Administrative Court in early 2024, but it had been varied on that point by the Supreme Administrative Court on the basis of the rule set out in section 36(8) of the 2007 Act that the Agency had no obligation to give reasons concerning points of fact when refusing requests for access to personal data (see paragraphs 43, 47 and 71 above).

B. The Court's assessment

284. The question of whether the proceedings for judicial review in respect of the Agency's refusal to disclose whether it had processed data relating to the applicants could furnish an effective safeguard against an arbitrary or disproportionate decision by the Agency on that point was reviewed in detail under Article 8 § 2 of the Convention (see paragraphs 248-252 above). The content of the applicants' submissions in relation to Article 13 of the Convention (see paragraph 283 above) demonstrates that they raised no further issue in relation to those proceedings.

285. There is, then, no need to examine the admissibility or merits of their complaint under Article 13 of the Convention (see, *mutatis mutandis*, *Yonchev v. Bulgaria*, no. 12504/09, §§ 32-33, 7 December 2017; *Negru v. the Republic of Moldova*, no. 7336/11, § 37, 27 June 2023; and *Kaczmarek*, cited above, § 101).

V. APPLICATION OF ARTICLE 41 OF THE CONVENTION

286. Article 41 of the Convention reads:

“If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party.”

A. Damage

1. The applicants' claim and the Government's comments on it

287. The two applicants claimed 1,000 euros (EUR) each in respect of the non-pecuniary damage that they had allegedly suffered as a result of the breaches alleged in the present case.

288. The Government contested the claim, pointing out that the applicants had not asserted that they had suffered any adverse consequences as a result

of the alleged breaches. In their view, a finding of a violation would amount to sufficient just satisfaction in respect of any breach found in the present case.

2. *The Court's assessment*

289. As attested by the adjective “just” and the phrase “if necessary” in Article 41 of the Convention, the Court enjoys discretion in the exercise of the power to afford such satisfaction to the injured party (see, as a recent authority, *Molla Sali v. Greece* (just satisfaction) [GC], no. 20452/14, § 32, 18 June 2020). In some cases, the public vindication of the wrong suffered by that party, in a judgment binding on the respondent State, can in itself amount to sufficient redress. This is especially so when, as here, (a) the finding of breach is based solely on the conclusion that a law, procedure or practice has fallen short of Convention standards (*ibid.*, § 33, with reference to *Varnava and Others v. Turkey* [GC], nos. 16064/90 and 8 others, § 224, ECHR 2009), without a further finding that this shortcoming has affected the applicants in any tangible way, and (b) general measures would constitute the most appropriate form of redress (see paragraph 4 of the Practice Direction on Just Satisfaction Claims, as amended in June 2022).

290. In the present case, no evidence has been produced to show that the refusal to inform the applicants of whether the Agency was processing data relating to them has caused them any tangible detriment. The applicants did not even specify the nature of the non-pecuniary damage that they had allegedly suffered on that account; since the first applicant is an individual and the second applicant a legal person, the nature of any such damage caused to them is, respectively, likely to be different. Even if it is accepted that they have both suffered some non-pecuniary damage on account of the absence of effective safeguards in relation to the potential processing by the Agency of data relating to their “private life” and “correspondence”, the finding of a breach of Article 8 of the Convention provides them sufficient just satisfaction in that regard (see, *mutatis mutandis*, *Amann*, cited above, § 94). It is, then, not necessary to award them any monetary compensation in respect of that.

291. It must at the same time be emphasised that under Article 46 of the Convention a judgment in which the Court finds a violation of the Convention or its Protocols imposes on the respondent State an obligation to choose (subject to supervision by the Committee of Ministers) the general and/or, if appropriate, individual measures to be taken in its domestic legal order to end the violation and make all feasible reparation for its consequences in a way to restore as far as possible the situation that would have obtained if the violation had not taken place. Moreover, it follows from the Convention, and from its Article 1 in particular, that in ratifying it the Contracting States undertook to ensure that their domestic laws would be compatible with it (see *Ekimdzhev and Others*, cited above, § 427).

B. Costs and expenses

1. The applicants' claim and the Government's comments on it

(a) The claim and the documents produced in support of it

292. The Committee sought reimbursement of a total of EUR 7,161.80 in respect of costs and expenses. It broke down its claim as follows:

(a) EUR 31.72 in respect of postage;

(b) EUR 230.08 in respect of court fees and costs paid to the Agency in the proceedings for judicial review of its first refusal to disclose the information sought by Mr Kanev (see paragraphs 12-27 above) and in the proceedings for judicial review of the Agency's official-secrets rule (see paragraphs 32-39 above); and

(c) EUR 6,900 in respect of fees for a total of sixty-nine hours of legal work on the case, at the hourly rate of EUR 100.

293. In support of its claim, the Committee produced:

(a) postal receipts;

(b) (i) two bank orders for the payment of a total of 140 Bulgarian leva (BGN – equivalent to EUR 71.58) in court fees for the proceedings for judicial review of the Agency's first refusal to disclose information (BGN 70 paid in respect of Mr Kanev and BGN 70 paid in respect of the Committee itself); (ii) three bank orders for the payment of a total of BGN 110 (equivalent to EUR 56.24) in court fees for the proceedings for judicial review of the Agency's official-secrets rule; and (iii) one bank order for the payment of BGN 200 (equivalent to EUR 102.26) to the Agency in respect of its own costs in the former proceedings;

(c) a time sheet for the work of its lawyer, Ms A. Kachaunova, on the proceedings for judicial review of the Agency's first refusal to disclose the information sought by Mr Kanev, the proceedings for judicial review of the Agency's official-secrets rule, and the proceedings before the Court; and

(d) a contract for legal services between Mr Kanev as a client and the Committee as a provider, in relation to the case before the Court.

(b) The Government's comments

294. The Government pointed out that there was no indication that two of the shipments in respect of which the Committee was claiming postage had concerned the present case. Furthermore, two of the five bank payment orders produced by the Committee were identical; one of them was therefore to be discounted, which meant that the proven amount of the sums paid in court fees and costs in the domestic proceedings was reduced the equivalent of EUR 194.29. Lastly, the legal services contract – which was between Mr Kanev and the Committee – concerned only Mr Kanev's representation before the Court. Nor did that contract duly define the hourly rate for the legal

services under it, or prove that Ms A. Kachaunova had been retained to represent the applicants domestically or before the Court. There was, moreover, no evidence that they had paid her any sums in respect of such work. She was not an employee of the Committee but a practicing lawyer, and was therefore only entitled to professional fees for her services, in accordance the provisions of the Bar Act 2004.

2. *The Court's assessment*

295. It is settled that (a) applicants are entitled to the reimbursement of costs and expenses only if they were actually and necessarily incurred and are reasonable as to quantum, and that (b) costs or expenses incurred to prevent the breach of the Convention or obtain redress for it through the domestic legal order are also recoverable under Article 41 of the Convention (see, among many other authorities, *Myumyun v. Bulgaria*, no. 67258/13, § 85, 3 November 2015; see also paragraphs 15 and 18-19 of the Practice Direction on Just Satisfaction Claims (as amended in June 2022)).

(a) Postage

296. The claim in respect of postage (see paragraphs 292 (a) and 293 (a) above) is to be allowed in full. The documents in the case file – and in particular, the correspondence sent to the Court by the applicants – show that all three postal shipments in respect of which the Committee claimed postage related to the present case. That postage, which came in total to BGN 62.04 (equivalent to EUR 31.72) is therefore to be awarded to the Committee in full.

(b) Domestic costs

297. The claim in respect of the court fees and costs paid in the proceedings for judicial review of the Agency's first refusal to disclose information – which came to BGN 340 (equivalent to EUR 173.84) (see paragraphs 292 (b) and 293 (b)(i) and (iii) above) – is to be allowed in full too. Those proceedings were an attempt by the applicants to – depending on how the matter is seen – prevent or obtain redress for the breach of Article 8 of the Convention. Contrary to what the Government contended, there is no duplication in two of the five bank payment orders produced by the Committee: one concerned a fee paid in respect of Mr Kanev and the other a fee paid in respect of the Committee itself (see paragraph 293 (b)(i) above); they were both claimants in those proceedings (see paragraph 12 above).

298. The claim in respect of the court fees paid in the proceedings for judicial review of the Agency's official-secrets rule (see paragraphs 292 (b) and 293 (b)(ii) above) must, by contrast, be dismissed. As noted in paragraph 223 above, the outcome of those proceedings did not affect the present case. Moreover, the claimant in those proceedings was solely

Mr Kanev (see paragraph 32 above), whereas the claim for costs and expenses under examination was made solely on behalf of the Committee (see paragraph 292 above).

(c) Lawyers' fees

299. The claim in respect of lawyers' fees (see paragraph 292 (c) above) must be dismissed as well. The Committee has produced no evidence that it has paid or is under a legal obligation to pay such fees to the lawyer who represented it domestically and before the Court, Ms Kachaunova – whether in its capacity as applicant or in its capacity as provider of legal services to Mr Kanev, in accordance with the contract between them (see paragraph 293 (d) above). The time sheet drawn up by Ms Kachaunova recording how many hours she has spent in work on the case does not in itself constitute proof of that. There is, then, no basis on which to accept that the lawyers' fees claimed by the Committee have been actually incurred by it (see *Merabishvili v. Georgia* [GC], no. 72508/13, § 372, 28 November 2017). Ms Kachaunova cannot seek just satisfaction on her own behalf, since a representative is not an “injured party” within the meaning of Article 41 of the Convention (see *Korporativna Targovska Banka AD v. Bulgaria*, nos. 46564/15 and 68140/16, § 223, 30 August 2022, with further references).

(d) Recapitulation

300. For all of the above reasons, the Committee is to be awarded a total of EUR 205.56, plus any tax that may be chargeable to it.

FOR THESE REASONS, THE COURT

1. *Declares*, by a majority, the complaint under Article 8 of the Convention admissible;
2. *Holds*, by five votes to two, that there has been a violation of Article 8 of the Convention;
3. *Holds*, unanimously, that there is no need to examine the admissibility or merits of the complaints (a) under Articles 10 and 11 of the Convention that the Agency had collected data about the applicants' political opinions, affiliations and activities, (b) under Article 10 of the Convention that the Agency refused to give information to the applicants, and (c) under Article 13 of the Convention;
4. *Holds*, by five votes to two, that the finding of a violation of Article 8 of the Convention amounts to sufficient just satisfaction in respect of any non-pecuniary damage suffered by the applicants;

5. *Holds*, by five votes to two,
- (a) that the respondent State is to pay the Bulgarian Helsinki Committee, within three months from the date on which this judgment becomes final, in accordance with Article 44 § 2 of the Convention, EUR 205.56 (two hundred and five euros and fifty-six cents) in respect of costs and expenses;
 - (b) that from the expiry of those three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period, plus three percentage points;
6. *Dismisses*, unanimously, the remainder of the claim for just satisfaction.

Done in English, and notified in writing on 28 April 2026, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Milan Blaško
Registrar

Ioannis Ktistakis
President

In accordance with Article 45 § 2 of the Convention and Rule 74 § 2 of the Rules of Court, the separate opinion of judges Pavli and Ní Raifeartaigh is annexed to this judgment.

JOINT DISSENTING OPINION OF
JUDGES PAVLI AND NÍ RAIFEARTAIGH

1. We have voted against the admissibility of the present applications, which we consider to be either manifestly ill-founded (in the case of Mr Kanev) or otherwise inadmissible (in the case of the Bulgarian Helsinki Committee – “BHC”). The information request which falls within the scope of the present case was the amended request filed on behalf of the applicants with Bulgaria’s State Agency for National Security (“the Agency”) at the end of June 2021 (see paragraph 8 of the judgment). Our main disagreement with the majority is that we do not consider this request to have been properly and clearly formulated as a request for access to personal data held by the Agency; on the contrary, it was phrased as a request for information about the use of intelligence methods. In our view, this has significant implications for the admissibility of the applications.

2. By way of context, we wish to point out, at the most general level, that data protection legal regimes and the laws governing the oversight of intelligence agencies have rather different origins and purposes. As the comparative surveys cited in the judgment itself make clear, intelligence operations tend not to be subject to data protection laws, at either national or supranational level, and data protection authorities have little or no oversight over them (see, especially, paragraphs 205-207 of the judgment). In so far as some data protection regimes do apply to intelligence services, this tends to be in relation to the personal data of their own personnel, rather than to third-party data collected through core intelligence functions. However, the safeguards related to surveillance or use of covert sources by security services tend to be *sui generis*, and have typically developed in *ad hoc* and incremental ways, reflecting the history, political system, institutional arrangements and other traits specific to each democracy. They come in many different shapes and colours. The Court has a well-developed case-law in this regard and has allowed the States a wide margin in terms of how they structure such safeguards in the national security and surveillance context, provided they meet the minimum standards developed under Article 8 of the Convention (see the case-law cited in paragraphs 241 and 243 of the judgment). Furthermore, these standards have themselves been developed by the Court with careful consideration for the special features of national security regimes. It may be noted that this case-law primarily locates remedies in respect of potential State abuse of intelligence methods in general measures such as clear legislation, independent supervision and other checks and balances in the system as a whole; there is not, for obvious reasons, any general individual right to know whether one has been the subject of a particular intelligence operation.

3. The domestic legal framework in the present case reflected this distinction both in terms of which bodies were entrusted with functions relating to personal data protection and intelligence oversight respectively, and the legal regimes governing those bodies. We consider that the manner in which the first applicant formulated the request which is the subject of the present case created confusion as to what he was actually seeking and renders his case inadmissible, for the following reasons.

The second applicant's request

4. Turning first to the request filed by the first applicant on behalf of the BHC, we note that the amended request to the Agency – in contrast to the original request filed earlier the same month (see paragraph 6 of the judgment) – did not include any references to the use of “special means of surveillance”, which relate essentially to covert interception of communications. (The first applicant's separate request to this effect filed with the National Bureau for the Oversight of Special Means of Surveillance – see paragraph 28 of the judgment – falls outside the scope of the present case.) As a legal entity, the BHC cannot claim an Article 8 interference with its “personal data”, but only its correspondence. As the amended request filed with the Agency in late June 2021 made no specific reference to the interception of its communications – and there being no actual indications before us that there might in fact have been such interceptions – we do not consider that the BHC can claim to be a victim of an interference with its Article 8 rights under the circumstances. The fact that legal entities are not entitled under national law to use the complaint procedure before the National Bureau does not change this conclusion. Nor do we consider that the mere theoretical possibility that BHC members might have been (lawfully) recruited as Agency informers under national law is sufficient to grant it victim status in the circumstances.

The first applicant's request

5. Turning now to Mr Kanev's request on his own behalf, we consider it important to highlight the precise terms of his information request. He asked whether the Agency's databases contained information on

(a) “any intelligence-gathering methods [that] had been used with respect to him” (see paragraph 8 of the judgment); or

(b) any BHC members who had been recruited as Agency informers.

6. Three points may be made about this request. First, it did not directly ask whether the Agency held personal data in respect of the applicant. Instead, it asked about the use of intelligence-gathering methods and the recruitment of informers (albeit in respect of him/the BHC and not those in use by the Agency in general). Secondly, such intelligence-gathering methods are

among the most sensitive aspects of any intelligence operations; as such, they tend to be granted the highest level of protection in classified information systems, for legitimate reasons. The same applies to the use of covert informers, for the protection of their safety and operating methods. Thirdly, the applicant's request made no reference to any possible illegality in the gathering of intelligence. The statements made by the Minister of Internal Affairs concerned possible abuses through the mass interception of communications (see paragraph 5 of the judgment), and we accept that this might have raised justified concerns among national civil society about potentially abusive deployment of other methods and techniques. Such concerns were not, however, spelled out in the request, and the Court must pay attention to the specific request actually made by the applicants which became the subject of analysis in the domestic judicial review proceedings.

7. Despite the absence of any explicit request as to whether the Agency held data in respect of the first applicant, the majority take the view that the request should nonetheless be treated, in substance or implicitly, as a personal data request. They do so on two grounds, both of which we view as problematic. The first ground is that they consider that the initial confirmation by the Agency might have “constitute[d] a necessary preliminary step for the exercise of any further rights or remedies” (see paragraph 217 of the judgment). In other words, they consider that the request actually made can be interpreted as a data request because it might have been a precursor to a data request. We are unable to share this conclusion and consider it unduly generous to the applicant. While it may be acceptable or understandable in the regular data protection context to simply ask for such confirmations as a first step in the procedure, this is not so straightforward in the national security environment (a point to which we return below). If the applicant wished to find out if the Agency held data in respect of him, there was no reason he could not have asked that question in plain terms. It not only was unclear but also brought him straight into the highly sensitive territory of secret methods and techniques.

8. The second ground offered by the majority for treating his request as a data request is the assumption that, if actually used, any intelligence-gathering methods would necessarily have resulted in the creation of Agency records containing personal data about the first applicant (see paragraphs 213-214 of the judgment). While this is possible, it is not necessarily or logically so. It is possible for a person to be subjected to surveillance measures without this resulting in any written records or other personal data being stored by an intelligence agency; this would be the case, for example, where human agents conduct surveillance of a group of people in a public place (say, at a protest), but without this resulting in the creation of any individualised records containing personal data. Again, we are unable to understand why the first applicant did not simply formulate the request as one concerning data held about him, if that is what he wanted to know.

9. The national Supreme Administrative Court held that the request did not properly seek access to any personal data held by the Agency, but had in effect concerned its intelligence-gathering methods (see paragraph 25 of the judgment). We cannot fault the national courts for not being as generous as the Chamber majority in “reinterpreting” the applicant’s request as a data protection request.

10. We return to the point that the applicant’s request did not contain any reference to unlawful use of surveillance techniques. We consider this to be a significant omission, because concerns or suspicions about being placed under unlawful surveillance clearly strengthen an applicant’s Article 8 claims to be informed of the nature and scope of such illegality. Conversely, there is no unconditional Article 8 right to be informed of the fact of surveillance *per se*, in the absence of any confirmed illegality. If surveillance is found to have been carried out lawfully, following a process that meets the Convention criteria for *ex post facto* review, the Court has accepted that the person may simply be informed that there has been no illegal surveillance, on a “neither confirm, nor deny” basis (see *Kennedy v. the United Kingdom*, no. 26839/05, §§ 95 and 167, 18 May 2010). (This is, incidentally, the same kind of response that the applicant received from the Oversight Bureau in the present case.)

11. The applicants have therefore invited the Court to find flaws in the overall domestic system of safeguards concerning intelligence methods in circumstances where the domestic litigation centred around a request which (i) was made to an intelligence agency not governed primarily by data protection law; (ii) at best, was ambiguous as to what information it was seeking, and at worst, simply asked for information about the use of intelligence methods; and (iii) did not differentiate between lawful and unlawful intelligence gathering despite this factor having significant implications in terms of Article 8 protection.

12. In view of the above considerations about the flawed nature of the first applicant’s amended request to the Agency, we consider that, even assuming that there has been an interference with his Article 8 rights – which is debatable –, the claim of a violation of that provision is manifestly ill-founded in the circumstances.

13. That being the case, it is not necessary for us to delve into the merits, but we do wish to make the observation that, having regard to the distinction between data protection regimes and legal frameworks governing State intelligence functions (as described in paragraph 2 above), we have concerns that the judgment blurs the line between the two situations and unnecessarily reinvents the Court’s methodological wheel for dealing with intelligence oversight. The existing case-law of the Court with regard to safeguards against abuse of intelligence methods is already adequate and there is no need to engage in an extensive analysis, for example, of EU data protection law.

KANEV AND BULGARIAN HELSINKI COMMITTEE v. BULGARIA JUDGMENT –
SEPARATE OPINION

Furthermore, the efforts to infuse ordinary data protection approaches into this area of Article 8 case-law are bound to create confusion and uncertainty.